



State of Israel

# **State Comptroller Report**

Cyber and Information Systems

---

## A b s t r a c t s



November 2024 | Jerusalem

Catalogue Number 2024-S-008

ISSN 0973-1948

[www.mevaker.gov.il](http://www.mevaker.gov.il)

Graphic Design: ER Design Team



# Table of Contents

## Abstracts

<b>Foreword</b>	5
-----------------	---

## Systemic Audits

Government Risk Management in the ICT	11
Ask Once Policy – Follow-up Audit	27

## Israel Postal Company

Information Systems at the Israel Postal Company and the Postal Bank	47
--	----

## The National Insurance Institute

Information Security and Cyber Protection at the National Insurance Institute	59
The Tevel Project for Upgrading the Computing Systems in the National Insurance Institute – Follow-up Audit	71

## Government Defense Industries

Cyber Security: Aspects of Regulation and Protection of the Information and Computer Systems at Rafael Advanced Defense Systems Ltd.	85
--	----

## Special Report

Artificial Intelligence – National Preparedness	93
---	----





## Foreword

**This report, which is placed on the Knesset's table, presents the results of the audit in the Cyber and Information Technology protection. It also includes a special report on the National Preparedness in the Artificial Intelligence.**

Since October 2023, the State of Israel is engaged in the Swords of Iron War, in the north and in the south, following the surprise murderous attack by the Hamas terrorist organization on the communities near the Gaza Strip and the surrounding area on Simchat Torah (celebrating the completion and rebeginning of the reading of the Torah) October 7th, 2023. As I have previously announced, our office is conducting a comprehensive audit on the matters concerning the massacre on October 7th and the Swords of Iron War. In my opinion, it is a public and moral duty to conduct an audit on the manner in which all the echelons functioned on the day of the massacre, during the period preceding it and during the period following it. Alongside with the audit on the war, our office is continuing to conduct audits in other areas as well.

In recent years, and in particular during the course of the war, we are witnessing an increase in cyber-attacks against the State of Israel carried out by states and great powers to damage and disable organizations. The Israel National Cyber Directorate has estimated the costs of dealing with the cyber-attacks in Israel during 2024 at about NIS 12 billion.

When I first took office as the State Comptroller and Ombudsman, I identified and defined the field of cyber as one of the core subjects that the State Audit will deal with. This is with the aim of examining the preparedness and readiness of the audited bodies to deal with the significant risks in the cyberspace, the strategic threats and future cyber challenges. My office's audits of cyber and information systems indicate the lack of relevant regulation in the cyber field, necessary to oblige organizations to take protection measures; the essential entities in the economy should be prepared to deal with attacks by states or great powers; and the decision makers within the government must be aware of the level of protection in the economy and its deficiencies. This report deals entirely with the results of the State Audit in the cyber and information systems protection. The chapters of the report are as follows:

- **The Government Risk Management in the ICT**
- **Ask Once Policy – Follow-up Audit**
- **Information Systems at the Israel Postal Company and the Postal Bank**
- **Information Security and Cyber Protection at the National Insurance Institute**



- **The Tevel Project for Upgrading the Computing Systems in the National Insurance Institute – Follow-up Audit**
- **Cyber Security: Aspects of Regulation and Protection of the Information and Computer Systems at Rafael Advanced Defense Systems Ltd.**
- **Artificial Intelligence – National Preparedness**

It should be noted that regarding the chapter on the Cyber and Data Protection in the National Insurance Institute and the chapter on the Aspects of Regulation and Protection of the Information and Computer Systems at Rafael Advanced Defense Systems Ltd. confidentiality measures were taken by the Knesset's State Control subcommittee, which decided not to submit them in their entirety before the Knesset but rather publish only parts thereof, under section 17 of the State Comptroller Law, 1958 [Consolidated Version].

The following is an overview of several chapters of the report:

- The digital transformation, which has been integrated into most of the government's work processes, presents opportunities to improve the effectiveness of the government's work and the provision of advanced services to the public, alongside new challenges and risks. During 2022, the scope of the financial activity in the government ICT was NIS 4.8 billion. Therefore, it is essential to manage the risks in this field in an organized and methodological manner. The audit on the subject of **the Government Risk Management in the ICT** indicates considerable gaps in the ICT risk management by the government, including the lack of an overall governmental overview regarding ICT risks; the failure of the National Digital Agency to reduce broad risks; partial reports by government ministries concerning their main ICT risks; and the absence of a main organized and systematic program for ICT risk management in the government ministries, including aspects of risk management regarding projects and broad and cross-cutting risk management – such as a shortage of manpower and difficulty in recruiting and retaining staff. As a result, 80% of the employees in the ICT in the government are freelancers (3,993 out of 5,308 employees during 2022).

The Israel National Cyber Directorate must address the findings of this audit and the government heat map of the areas of risk in the ICT presented in the audit report, to focus the government activity in this field and ensure that the risk management in this challenging and dynamic field is performed methodologically and optimally and allows preparation for the challenges in advance, providing a solution for the changes occurring in the environment of the government activity.

- The Israel Postal Company was a government company under the full ownership of the State of Israel (until it was privatized in May 2024), providing postal services as well as banking services via its subsidiary – the Postal Bank. As of the end of 2023, the Postal Company and the Postal Bank have 400 postal units, 650 collection centers and about 60 regional postal centers. During 2023, about 11.9 million customers of the Company



and the Bank received services in the postal units. The Postal Company has 55 information systems, some of which are divided into sub-systems, and the Postal Bank has 16 additional systems, some of which are divided into sub-systems, and the annual average of the operational expenses and the investments of the Information Systems Department is NIS 124 million. These systems are based on various technologies and supported by over 20 suppliers. The audit on the **Information Systems in the Israel Postal Company and the Postal Bank** found deficiencies in the information systems and data protection in the Postal Company and the Postal Bank, including poor management of the procedures for revoking authorizations for employees and its monitoring – thus, 85 (3%) of authorizations holders for a particular system are not defined in the human resources system as "active" and also 79 of them were not located in the Company's computerized controls, 780 (about 13%) of the holders of the active authorizations in the network's central management system are employees who are not included in the list of active employees in the Company's human resources system; the use of outdated automated equipment which is detrimental to both the service provided to the Company's customers and the Bank and the data protection – thus, despite the project for replacing the automated equipment being already defined as a strategic project in 2019, the Postal Company started to replace it only at the beginning of 2022. Until March 2024, only 683 out of 1,850 computers had been replaced or upgraded; the lack of a multi-year work plan for the Information Systems Department; the lack of monitoring and follow-up of the performance of the work plans; the multiplicity of information systems that makes it difficult to transfer the information between those systems and requires the performance of manual procedures and the investment of resources to compensate for this.

The Information Systems Department at the Postal Company must determine a methodological plan that includes the development of the information systems from a future standpoint, the upgrading of old systems and the optimization of the existing systems and the integration between them; while ensuring cyber protection and the reduction of exposure to risks originating in the various aspects of unauthorized use. The Postal Company must, as part of the process to improve data protection – and in particular in light of the cyber incident that occurred there in April 2023 – to improve the control over the of Company's authorization management. The Company must examine the deficiencies that were raised in the audit and immediately rectify them.

- The report includes a chapter on the **Cyber Protection: Aspects of Regulation and Protection of the Information and Computer Systems at Rafael Advanced Defense Systems Ltd.** In 2022, the budget allocated to the Cyber and Technology Protection Department at Rafael constituted 10% of the computing budget of the Information Technologies and Processes Administration. Additionally, the rate of phishing incidents reported to the Israel National Cyber Directorate in 2022 represented 31% of the total 9,108 cyber incidents recorded to it that year. The audit identified several deficiencies, including the lack of regulation of the working relationship between the



National Cyber Directorate and the Director of Security of the Defense System, as well as deficiencies pertaining to the protection of information and computer systems at Rafael. It is imperative that Rafael's management and board of directors address these deficiencies and collaborate with the Director of Security of the Defense System to ensure compliance with its directives, as required, given that Rafael's operations are a significant component for the enhancement of the country's military strength and resilience.

- My office conducts follow-up audits to examine whether the deficiencies indicated in the audit reports have been rectified. This report includes the follow-up audits regarding: **The Tevel Project for Upgrading the Computing Systems in the National Insurance Institute** – the follow-up audit indicated that most of the core deficiencies that arose in the previous audit had not been rectified or had been slightly rectified. This is notwithstanding that until the completion of the audit, public funds had been invested in the Tevel Project at over NIS one billion (more than twice as much as the Project's initial overall budget). It was further found that improving the service provided to the public and assisting the public in ensuring its rights had been achieved only partially, among other things due to a reduction in the Project's capacities; **Ask Once Policy** – the follow-up audit found that although since the completion of the previous audit there had been progress in the preliminary activity required for the implementation the Ask Once Policy – most of the deficiencies found in the previous audit had not been rectified with regard to the mapping of the government services provided to the public and an analysis of their characteristics. Although eight years have passed, the government plan resolved upon by the government in 2016 has not yet been fully implemented and the completion of the process is not expected in the next few years. The root of the problem is that the Digital Agency lacks the authority to oblige the government ministries to implement its directives. This, alongside with the lack of engagement of the government and public bodies in implementing those directives, lead to a partial implementation of the Ask Once Policy.
- In addition to the previously detailed chapters of the report, it includes a special report on **The National Preparedness in the Artificial Intelligence**. Preserving the State of Israel's supremacy in the domains of science and technology is a fundamental pillar of its national security, economic resilience, and the well-being of its citizens. This approach strategically compensates for the lack of natural resources and limited human resources compared to other countries. The artificial intelligence revolution is no longer a futuristic concept – it is an innovative core technology that increasingly influences various facets of contemporary life and emerges as a central element of competition in the international arena across a variety of fields: science, economy, industry, security, health, education, and employment.

The report indicates that the State of Israel already recognized in 2018 that the technological sector is on the brink of a significant revolution, and the Prime Minister acknowledged the necessity of preparing and implementing a comprehensive national plan on the subject. However, the government has not succeeded in leading and





executing a broad, comprehensive, and long-term national plan, and implement it, resulting in a decline in Israel's position in international benchmarks attesting to its readiness in the artificial intelligence. While the state has identified and analyzed the need in time, for several years it has failed in the decision-making and implementation stages.

To preserve Israel's technological and scientific superiority in the artificial intelligence, deemed a national priority, the Ministry of Innovation, Science, and Technology must guide the government's policy in this field under the government's resolution and the conclusions of the former Minister of Innovation, Science, and Technology in collaboration with the National Security Council. This includes, formulation of the national strategic plan, which was initiated in 2022. Additionally, the Ministry must establish a framework for periodic evaluation of compliance with the established goals in the plan, alongside individual assessments of the defined action directions and necessary updates. Moreover, it is imperative to examine the current management of implementing the approved measures under government resolutions, by parties acting voluntarily and without designated budgetary authority. At this juncture, the Ministry of Innovation, Science, and Technology must assume its responsibilities to ensure that the government's resolution is carried out as required. A clear leadership approach for a significant national program is crucial to maintain technological capabilities and relative advantages over other nations. Any deviation from the prescribed implementation path will necessitate a government update to assess the situation and provide responses to advance artificial intelligence as a government priority. It is recommended that the Prime Minister, who initiated the promotion of a national program in artificial intelligence already in 2018 as a basis for the government's resolution, monitor the government's progress through the National Security Council to ensure the practical implementation of a significant national plan.

**It is my pleasant duty to thank the employees of the Office of the State Comptroller, who work devotedly in conducting an audit professionally, intensively, thoroughly and fairly and in the publication of objective, effective and relevant audit reports.**

The State Comptroller's Office undertakes to continue auditing the audited bodies' compliance with current and future risks and engaging in cyber defense Information technologies and privacy protection for the benefit of Israeli citizens.



## Foreword

---

We will continue to pray and hope for the victory of the IDF and the Defense System in this difficult war forced upon us by our most bitter of enemies seeking to destroy us as a nation and as a state, for the return of the hostages to their homes, the return of residents from affected areas in the south and the north to their homes, the recovery of the injured and for peaceful and routine days.

A handwritten signature in black ink, appearing to read 'Matanyahu Englman'.

**Matanyahu Englman**  
State Comptroller and  
Ombudsman of Israel

Jerusalem, November 2024



Report of the State Comptroller of Israel – Cyber and  
Information Systems | November 2024

Systemic Audits

---

# **Government Risk Management in the ICT**





# Government Risk Management in the ICT

## Background

Digital technologies within government ministries are the core infrastructure for all governmental operations and a central means of managing and operating the ministries and providing service to the public. These ministries face various, including ICT<sup>1</sup> risks, impacting their operations and capacity to achieve their objectives.

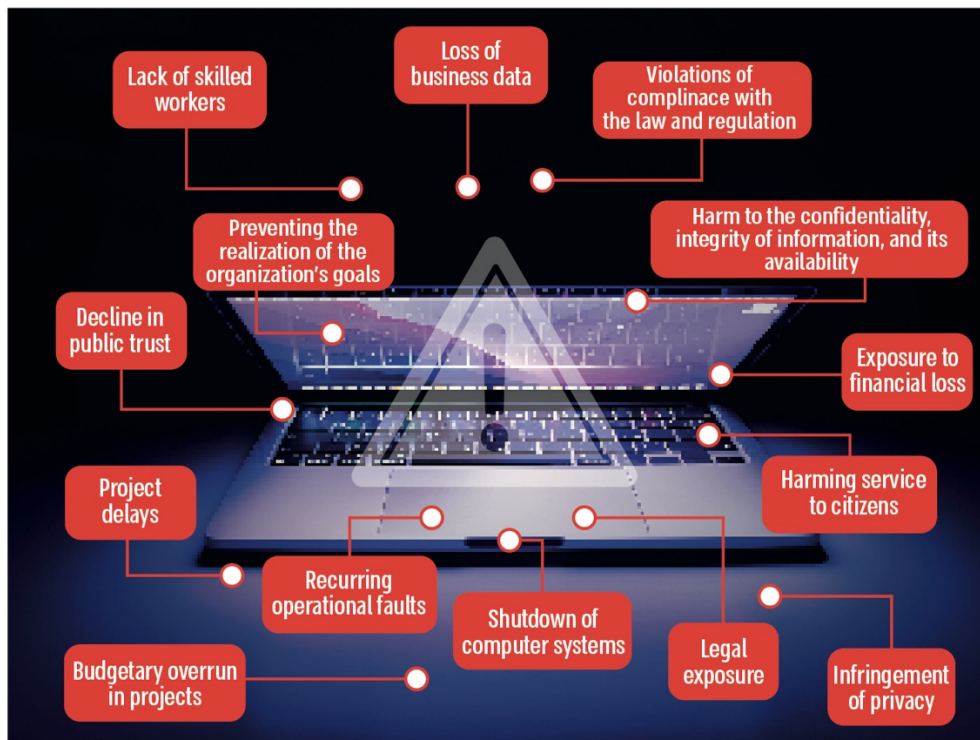
The necessity for ICT risk management in government is anchored in the government resolution from 2014<sup>2</sup>, the National Digital Agency guidelines<sup>3</sup>, the Financial and Economic Regulations (TAKAM) directives issued by the Accountant General at the Ministry of Finance<sup>4</sup>, and recognized international methodologies.

Implementing a structured and systematic approach for identifying ICT risk hotspots to which the ministry is exposed, assessing the implications and probabilities of these risks, preparing a comprehensive plan to mitigate or reduce them, and establishing a control system for early alerts regarding potential risk realization is essential to minimize the possible risks or their likelihood, and to prevent certain risks from materializing.

- 1 ICT risk – exposing ICT infrastructures, ICT processes or ICT projects to a failure event that could harm the organization and its goals, damage information, damage the level of service or lead to failure to meet mandatory standards.
- 2 Government Resolution 2097 (October 10, 2014).
- 3 As of 2023, 48 bodies – government ministries and auxiliary units – are guided by the National Digital Agency (government ministries).
- 4 Financial and Economic Regulations (TAKAM) directive 5.2.1 "Principles for managing operational risks at headquarters divisions in the Accountant General's Division and in the accounting departments of government ministries".



## Potential Damage Due to Realization of ICT Risks





## Key Figures

**NIS 4.8 billion**

the government's ICT financial activity in 2022

**80%**

of government ICT workers are service providers (3,993 out of 5,308 in 2022), posing various risks to the recruitment and retention of personnel

**X**

the National Digital Agency did not formulate a government situation report of ICT risks nor reduce wide-ranging risks

**for about 2.5 years**

no Chief ICT Risk Manager has been appointed by the National Digital Agency (2021– 2023)

**about 65%**

of government ministries that reported in the "Itam"<sup>5</sup> system in 2022 (24 out of 37) noted that human capital is a key risk

**about 57%**

of government ministries that reported in the "Itam" system in 2022 (21 out of 37) noted that the budget is a key risk

**8 ministries**

of the 13 audited ministries (62%) had not appointed, as of July 2023, a ministry ICT risk manager

**8 ministries**

of the 13 audited ministries (62%) did not conduct a comprehensive organizational risk survey

5 A central information system for managing technological governance processes developed by the National Digital Agency.



---

## Audit Actions



From November 2022 to August 2023, the State Comptroller's Office audited the management of ICT risks within the government. The audit examined the operations of the National Digital Agency for ICT risk management, the mapping of ICT risks at the national level, and the management of ICT risks across government ministries and auxiliary units. The audit was carried out in the National Digital Agency at the Ministry of Economy and Industry. Completion examinations were conducted in the DIT divisions (Digital and Information Technologies Divisions) across 13 ministries and auxiliary units supervised by the National Digital Agency. These included the Ministry of Finance, the Ministry of Justice, the Ministry of Education, the Ministry of Health, the Ministry of Foreign Affairs, the Ministry of Environmental Protection, the Ministry of Communications, the Ministry of Agriculture and Rural Development, the Ministry of Welfare and Social Affairs, the Enforcement and Collection Authority, the Population and Immigration Authority, the Ministry of Economy, and the Central Bureau of Statistics.

The audit focused on the ICT risk management processes regarding the development of central applications, the operation and maintenance of systems, facilities, and physical infrastructure, the procurement of equipment and software, and human capital, constituting most of the financial activities in this area (92%). Risk management concerning information and cyber security<sup>6</sup> was not examined.

---

## Key Findings



**Appointment of a Chief ICT Risk Manager in the National Digital Agency** – from the end of 2020 until August 2023, the National Digital Agency did not appoint a Chief ICT Risk Manager, as required by the government resolution of 2014. This adversely affected the Agency's capacity to lead and guide DIT (data, information and technology) divisions within government ministries on ICT risk management and assist them in conducting ICT risk surveys and implementing risk mitigation plans. The absence of a Chief ICT Risk Manager also hindered the formulation of a comprehensive government situation report on ICT risks, deploying ICT risk management methodologies across government ministries, and promoting collaborative efforts to mitigate these risks.

---

<sup>6</sup> According to a government resolution from 2014, in all matters relating to cyber defense, the Chief ICT Risk Manager will be professionally guided by the Government Cyber Defense Unit (Yahav).





**Coordination of the Government Situation Report of ICT Risks and Initiating Lateral Activities to Reduce the Risks** – despite the 2014 government resolution assigning the National Digital Agency the responsibility for coordinating the government situation report of ICT risks and initiating lateral activities to reduce the risks, the following were found:

- The National Digital Agency did not form a cross-government situation report of ICT risks from 2021 to 2023, despite reports from several ministries in the "Itam" system during this period about their primary ICT risks. Since 2014, the ministry-wide ICT risk mapping was conducted only once, in 2019.
- The National Digital Agency has not monitored the evolution of ministry-wide risks within the government over the years nor tracked their levels and any changes.
- The National Digital Agency failed to mitigate lateral risks in 2022–2023 despite the obligations outlined in the government resolutions and receiving reports from ministries about the primary ICT risks they encountered.
- Knowledge retention within the National Digital Agency concerning managing ministry-wide ICT risks across the government is insufficient.

**Government Ministries' Reporting on Ministry-Lateral ICT Risks** – in formulating work plans, DIT divisions within government ministries were directed by the National Digital Agency to specify in the "Itam" system three to five primary risks that impact their capacity to meet their objectives. The following was found:

- In 2022 and 2023, about 20% of the 48 ministries guided by the National Digital Agency failed to report any ministry-wide ICT risks. In 2022, the ministries rate that did not report at all was 23% (11 ministries); In 2023, this rate decreased to 19% (9 ministries).
- Some government ministries submitted only partial reports, detailing one or two risks: In 2022, 40% of ministries reported partially (19 ministries). This increased in 2023, with 50% of ministries providing partial reports (24 ministries).

Consequently, in 2022 and 2023, 63% of ministries (30 ministries) and 69% of ministries (33 ministries), respectively, failed to comply fully with reporting requirements regarding ICT risks in the "Itam" system. The lack of comprehensive reporting by most ministries undermines the National Digital Agency's ability to create an accurate government situation report of ICT risks, analyze their implications, and devise ministry-wide actions and strategies for mitigation.

**The National Digital Agency Reporting on Ministry-Lateral Risks** – the National Digital Agency, responsible for the development of national digital services and technological infrastructures, was the only entity among the 48 ministries that did not utilize the "Itam" system for reporting ministry-wide ICT risks from 2021 to 2023. This



raises concern, particularly given the Agency's role as a benchmark for other government ministries.

**📌 Reporting on Project-Level Risks** – an analysis of reporting practices between 2021 and 2023 raised that between two and 11 ministries out of 48 failed to report project-level risks each year.

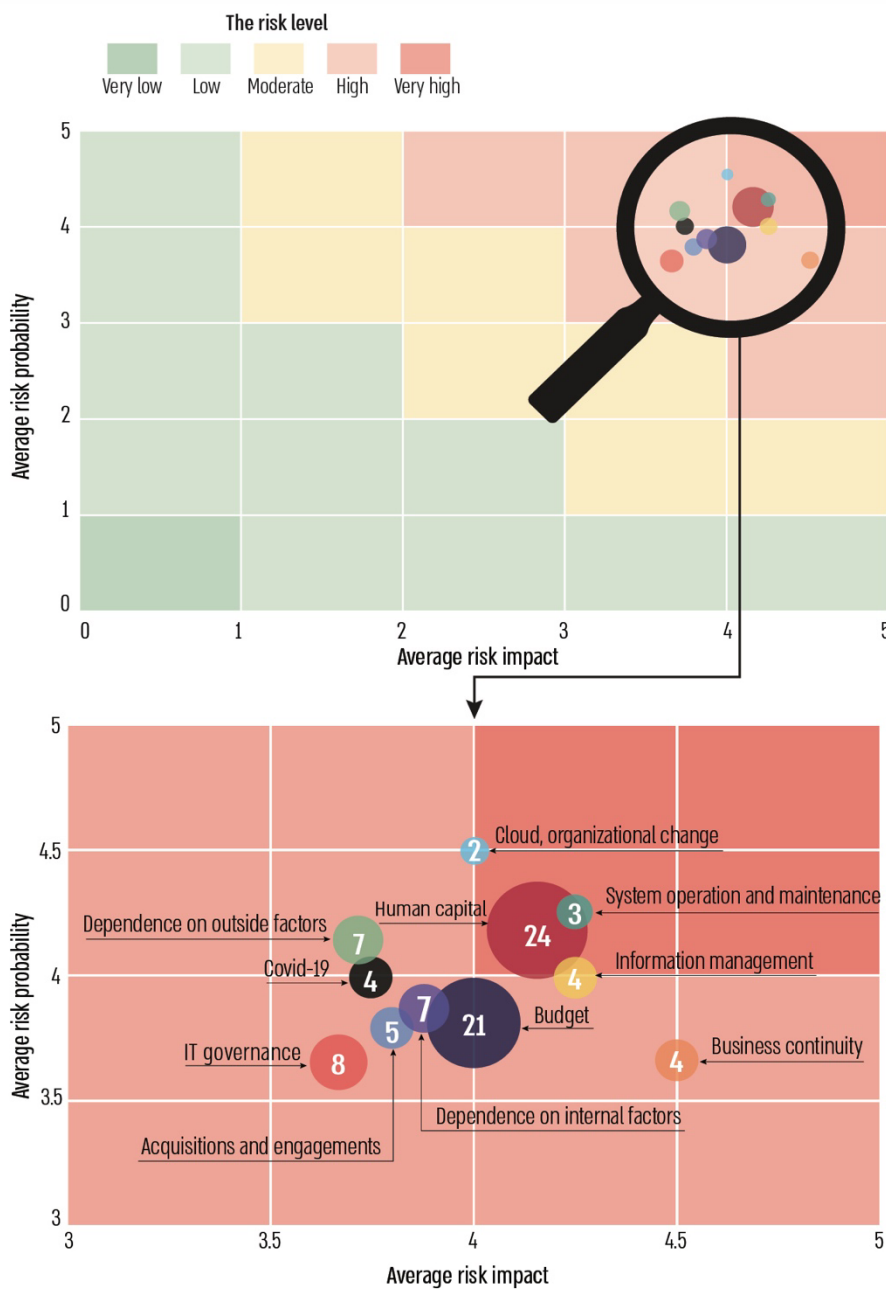
**📌 Assessing Government's ICT Risk Situation Report** – due to the National Digital Agency's failure to provide an updated situation report of ICT risks, the State Comptroller's Office conducted an analysis based on partial data from reports submitted by 37 government ministries through the "Itam" system, to identify ministry-lateral risks reported in 2022 and clarify the overall risk situation report:

- **Frequency of Reporting on Each Risk** – in 2022, the ICT risk most frequently reported by ministries was human capital, noted by 65% of ministries (24 out of 48). This encompasses issues such as inadequate standards, workforce shortages, insufficient employee skills, retention challenges, and recruitment difficulties. Additionally, budget-related risks were highlighted by over half of the ministries (57%, or 21 ministries), which include concerns such as the absence of an approved state budget and the partial funding of projects not included in the budget base. IT governance risks were noted by about 20% of ministries, indicating discrepancies between DIT division work plans and organizational business needs.
- **Risk Level Reporting** – the human capital risk was reported 22 times at high and very high-risk levels, describing a significant potential for damage with both high impact and likelihood of occurrence. The budget risk was reported 13 times at similar severity levels.

The State Comptroller's Office utilized a heat map to represent these risks visually. The color coding indicates risk levels: high risk is expressed in red, moderate risk in yellow and low risk in green. Each circle within the diagram represents a particular risk category; Its X-axis position illustrates the average impact of the risk, while the Y-axis indicates the average probability of risk occurrence. The size of each circle and the numbers contained within indicate the number of ministries that reported the respective risk.

The upper section of the heat map below displays the distribution of risks, while the lower section offers a focused view of high to very high-risks and the number of ministries reporting those risks.

## The Government Heat Map of ICT Risks, According to Reports in 2022 in the "Itam" System



According to the reports of the ministries in the "Itam" system, analyzed and processed by the Office of the State Comptroller.



The heat map indicates that all identified risks fall within a high to very high-risk category. This classification denotes the potential for significant damage with a high likelihood of occurrence. They are the most prominent risks, not only in the frequency of reports on them, but also in the high level of investigated risk. This heat map, derived from partial ministry reports, can guide the Agency and relevant government ministries in focusing their efforts on ICT risk mitigation, prioritize actions and resource allocation to address these risks.

**📌 Appointment of ICT Risk Managers in Ministries** – as of July 2023, eight out of the thirteen audited government ministries (62%) have not appointed an ICT risk manager, as required, including the Ministry of Education, the Population Authority, the Ministry of Agriculture, the Ministry of Communications, the Ministry of Foreign Affairs, the Ministry of Economy and Industry, the Ministry of Environmental Protection, and the Ministry of Welfare. Furthermore, the National Digital Agency lacked information regarding the appointment of these risk managers despite its mandate to maintain ongoing communication with ministries and receive updates on risk survey findings, material risks, and the progress of treatment plans.

**📌 Conducting a Comprehensive ICT Risk Survey at Ministries** – an examination conducted in 13 ministries regarding the execution of a comprehensive ICT risk survey, which maps the primary risks associated with the ministry's ICT activities and prioritizes their addressing, raised that:

- Three ministries – the Ministry of Justice, the Ministry of Health<sup>7</sup>, and the Ministry of Education, which are obligated by the National Digital Agency's guidelines to undertake a thorough organizational ICT risk survey due to their annual financial activities exceeding NIS 250 million<sup>8</sup>, have failed to conduct such surveys in the past four years. In 2022, the Ministry of Health's ICT financial activity was NIS 550 million, the Ministry of Justice's NIS 466 million, and the Ministry of Education's NIS 358 million.
- The Ministry of Justice – significant ICT risks were identified, including challenges related to cloud transition, personnel retention, and budget constraints. These risks affect the DIT Division's objectives, ranging from damage at the organizational unit level to the Ministry's overall goals. The Ministry of Justice has presented risk assemblage and specific mitigative measures to the State Comptroller's Office. However, these do not nullify a comprehensive ministry ICT risk survey as mandated by the National Digital Agency's guidelines nor facilitate informed decisions for addressing critical risk exposure.

---

<sup>7</sup> The examination at the Ministry of Health does not encompass the Medical Centers Division.

<sup>8</sup> According to data held by the National Digital Agency, "Overview of the government ICT activity 2022".



- The Ministry of Education – the Ministry of Education faced various significant ICT risks, including human capital, cloud transition, and the maintenance of outdated core systems. It has been noted that, despite the National Digital Agency's guidelines mandating a comprehensive organizational risk survey, the Ministry has not conducted such a survey in recent years. While some mitigation actions have been implemented to address specific known risks, this does not negate the necessity for a thorough ICT risk survey to identify and map additional material risks, along with a detailed mitigation plan to address them effectively.
- The Ministry of Health – the Ministry of Health is encountering considerable risks and organizational challenges in ICT, including human capital, the transition to cloud infrastructure, outdated systems, budget constraints, and more. While the Ministry has developed a strategic plan to address these challenges, the plan lacks a detailed analysis of the associated risks and their significance, mitigation actions, and defined timelines for resolution. Furthermore, the Ministry has not performed a thorough organizational risk assessment in recent years, despite this being a requirement according to the National Digital Agency's guidelines.
- Of the ten other audited ministries, whose annual ICT activities were less than NIS 250 million but still represent significant financial involvement, five ministries (50%) – including the Ministry of Welfare, the Ministry of Finance, the Ministry of Economy, the Ministry of Agriculture, and the Ministry of Communications – have not executed a comprehensive organizational ICT risk survey in recent years, despite recommendations from the National Digital Agency for all units to do so regardless of the financial scope of their activity.
- As of August 2023, the National Digital Agency has not compiled a comprehensive mapping of government ministries and auxiliary units that have conducted thorough risk surveys, despite existing guidelines mandating ministries report findings, material risks, and progress of plans for addressing them to the Chief ICT Risk Manager.

**🔴 Risk Management in Projects** – it has been found that ICT risk management within the audited government ministries is often not conducted in alignment with the guidelines set forth by the National Digital Agency, nor systematically and continuously throughout the project life cycle. Additionally, it frequently lacks vital elements such as defining the level of risk and its implications, establishing a timeline for implementing mitigation actions, monitoring outcomes to determine whether the risk has been mitigated or expanded, and assessing the effectiveness of the mitigation measures.

**🔴 Risk Management in the National Digital Agency** – the National Digital Agency has not undertaken a comprehensive organizational ICT risk assessment as mandated by its guidelines, despite this being necessary due to its substantial financial engagement in



the ICT sector – at NIS 446 million annually – and its responsibility for managing critical core systems in the government's ICT sector.






**Formulation of a Policy and Methodology to Manage ICT Risks and Assisting to Implement Them** – over the years, the National Digital Agency has established a policy for managing ICT risks and implementing the corresponding methodology, which includes publishing guidelines and providing training for ministries. A National Digital Agency audit indicated that adopting these guidelines and methodology within the ministries is inadequate. To ensure optimal ICT risk management in government ministries, it is recommended that the Agency enhance its training and implementation efforts and explore additional actions necessary for the effective execution of ICT risk management processes in government offices.

**Establishment of the "Itam" System** – the National Digital Agency established the "Itam" system, a centralized information system for managing technological governance processes. This system incorporates a module for managing ICT risks, wherein a risk management methodology is applied. This methodology utilizes a central risk bank containing a list of typical and relevant ICT risks applicable to government ministries. The bank's objective is to efficiently, comprehensively, and promptly identify ICT risks, maintain consistency in risk mapping, and facilitate cross-cutting analyses of ICT risks across government ministries.

---

## Key Recommendations

-  The National Digital Agency should map and analyze organization-wide ICT risks, update the cross-government ICT risk map, and continuously monitor risk levels. It is recommended that this map be integrated into the annual government-lateral situation picture regarding ICT activities. Furthermore, the National Digital Agency should initiate organization-wide measures to mitigate these risks and report its actions for risk mitigation to the government ministries.
-  For the National Digital Agency to comply with the government resolution, formulate a comprehensive picture of all ICT risks, and mitigate them, it should ensure all government ministries report in the "Itam" system, including ministry-lateral and project-specific risks. This requires refining and clarifying reporting guidelines to achieve a complete situational report.
-  Ministries that have not appointed a ministry ICT risk manager should prioritize the appointment of this role promptly. The National Digital Agency should also supervise this process to confirm that all ministries appoint such positions.



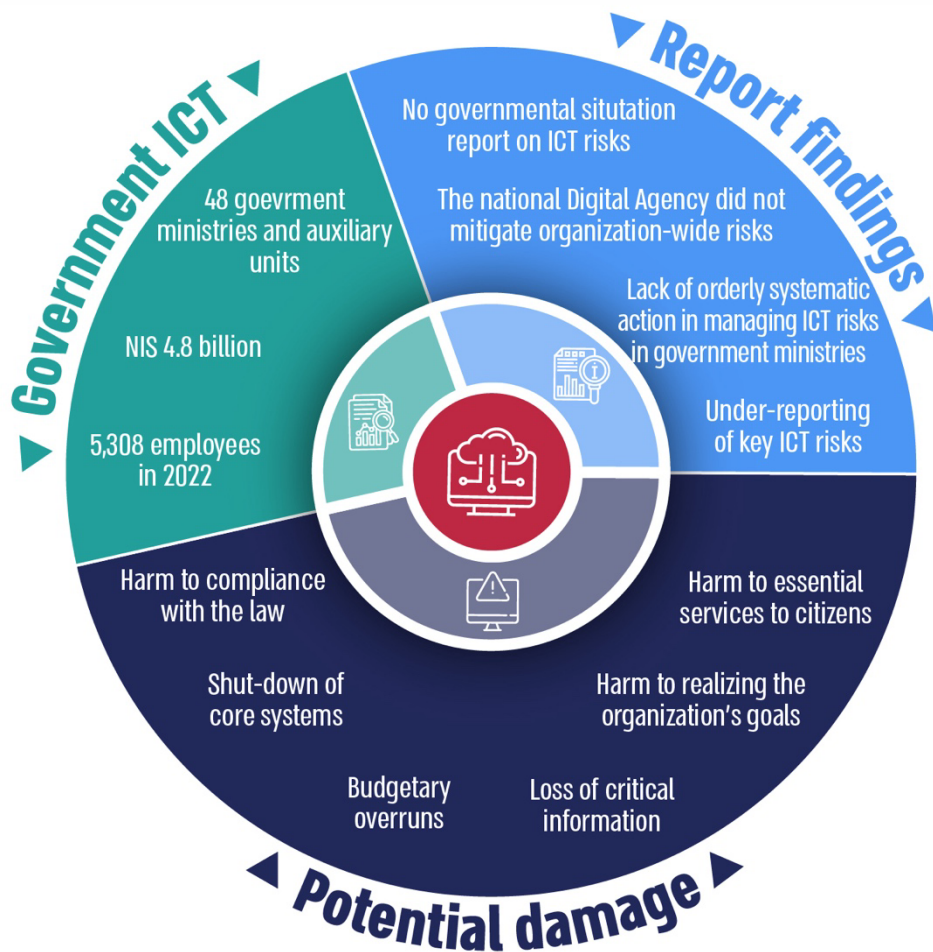
- 💡 Ministry ICT risk managers should maintain a consistent risk management routine, including a work plan for risk assessments and the development of an annual plan for managing ICT risks.
- 💡 It is recommended that the National Digital Agency monitor the ministries' execution of risk assessments and adherence to established mitigation plans. Additionally, the Agency should consider lowering the threshold requiring organizational ICT risk surveys for ministries with annual ICT financial activities below NIS 250 million.
- 💡 The National Digital Agency should map and analyze systemic risks affecting all facets of technology and digital transformation within the government, particularly evaluating risks linked to the non-adoption of new technologies<sup>9</sup>, and formulate a comprehensive long-term management policy. This should include identifying organization-wide ICT risks raised by government ministries.
- 💡 Finally, the National Digital Agency should enhance its initiatives regarding implementing risk management methodologies within the ministries.

---

9 RONI-Risk Of Not Investing



## Government Risk Management in the ICT – Summary Chart







---

---

## Summary

Digital transformation and its integration into government work processes present opportunities for improving efficiency and enhancing public services, along with new challenges and risks. It is, therefore, essential to manage ICT risks within the government systematically and methodically.

This report identifies significant gaps in ICT risk management in the government, including the absence of a centralized situation report of ICT risks, inadequate actions taken by the National Digital Agency to mitigate organization-wide risks, insufficient reporting from government ministries on critical ICT risks requiring attention, and the lack of a centralized, systematic approach to managing ICT risks across ministries, including both inter-ministerial risk management and risk management within ICT projects.

The National Digital Agency should consider the findings of this report and the accompanying government heat map of ICT risks to prioritize relevant efforts. This will ensure that risk management in this complex and dynamic field is conducted effectively, allowing for proactive preparation for challenges and responsive adaptation to changes in the environment of governmental activity.





Report of the State Comptroller of Israel – Cyber and  
Information Systems | November 2024

Systemic Audits

---

# **Ask Once Policy – Follow-up Audit**





## Ask Once Policy – Follow-up Audit

### Background

The executive authority, through its various branches, provides many services to the public. One of the ways to streamline the services provided by government ministries and auxiliary units to the public is the provision of services in a wholly digital format from end to end in one place in a friendly and accessible manner while implementing the "Ask Once Policy," which means **receiving information<sup>1</sup> from the citizen only once and sharing it between government bodies to facilitate the provision of various services without the need for repeated submissions by citizens.**

In 2016, the government adopted the Ask Once Policy across ministries and auxiliary units to enhance public service delivery and reduce bureaucratic burdens (Resolution 1933<sup>2</sup>). This resolution mandates that government ministries share necessary information to improve public services, adhering to restrictions and guidelines outlined in the resolution and applicable laws. For instance, the guidelines balance information sharing for optimized service delivery and the obligation to maintain privacy under the Protection of Privacy Law, 1981, mindful of the sensitivity, scope of information, and the public benefit derived from such sharing. In 2020, amid the Covid-19 pandemic, the government initiated a plan to accelerate digital services to the public (Resolution 260<sup>3</sup>). This plan involved the then-Ministry of Cyber and National Digital Matters and about 40 additional ministries and public bodies in driving significant reforms in bureaucratic processes through advanced digital solutions and wide technological platforms, including alleviating bureaucratic burdens via the Ask Once Policy.

To successfully implement the Ask Once Policy on a large scale within government services, it is imperative to identify and map the services offered by each ministry, validate these services by analyzing their characteristics, including required references and agencies involved, incorporate them into a comprehensive database cataloging all government services; connect them to the government's technological infrastructure that enables information sharing and approve the transfer of information between the bodies in the

- 1 Data stored on a government database or confirmation issued by a government ministry.
- 2 Government Resolution 1933, "Improving the transfer of government information and making government databases accessible to the public" (August 30, 2016).
- 3 Government Resolution 260, "Plan to accelerate digital services for the public and promote digital literacy and amend a government resolution" (July 26, 2020).



Information Transfer Committees<sup>4</sup>. In line with Resolution 1933, the National Digital Agency<sup>5</sup> established the Information Highway, a secure infrastructure for information transfers between government ministries and public bodies, along with a "committee system" (Moed system) to facilitate the management and authorization of these processes.

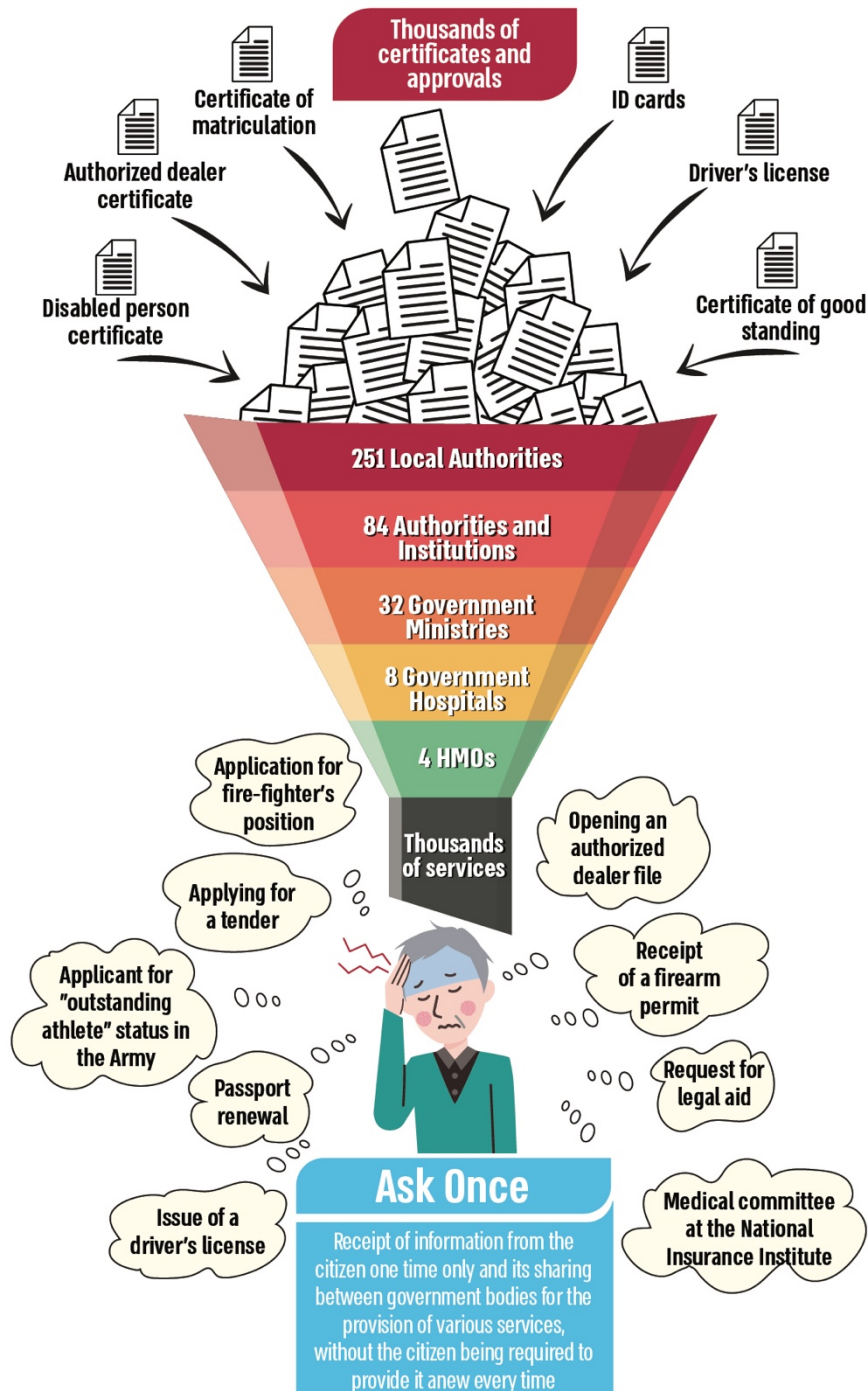
This report was written in light of the "Iron Swords" War and the civilian response given to the population during the months of conflict since October 7. The significance of providing digital services to citizens is amplified during emergencies. Information transfer between public bodies is crucial for effective government operations and public service provision during emergencies, particularly regarding critical and life-saving services. Throughout the Iron Sword War, numerous citizens and businesses required various government services, including support for families of the hostages, the missing, and the fallen, assistance for those whose property suffered damage, aid for evacuees, services for individuals whose livelihoods were impacted, and firearms licensing. Efficient online services can alleviate the emotional distress of those affected and optimize the time and resources involved in submitting applications and exercising rights within various government ministries.

---

4 According to Regulation 3A of the Protection of Privacy (Information Security) Regulations, 2017, every public body that provides or receives information is required to appoint a committee whose duty is to discuss requests for the provision of information from the ministry to public bodies or requests by the ministry to receive information from another public body and to consider whether to approve these requests.

5 The National Digital Agency was established in 2021 in the course of the merger of the Government ICT Authority and the Headquarters of the Israel Digital National Initiative.

## Illustration of the Ask Once Policy





## Key Figures

**?**

about eight years after the implementation of the Ask Once Policy in the government and the auxiliary units, the National Digital Agency still does not have data regarding the scope of services in which this policy is implemented

**in only  
9%**

of the government services (350 out of 3,888), the Information Highway<sup>6</sup> is used for information transfers between government ministries and public bodies

**342 days**

on average, in 2023, were required to approve or deny a request to transfer information between public bodies. Almost six times longer (570%) than the time set in the government resolution – 60 days

**240,000**

firearms licensing applications were awaiting review by the Ministry of National Security during the war (as of December 2023). Still, only in April 2024, a digital interface was established between the IDF and the Ministry of National Security to transfer the information required between them to advance the review of applications

**0**

of the 480 services provided by the Ministry of Education have been validated; hence, it is impossible to know which ones are suitable for implementing the Ask Once Policy

**0**

meetings of the Steering Committee on Information Transfers between Public Bodies were convened in 2021–2023

**0**

of the Ministry of Defense services relevant to bereaved families and disabled IDF personnel are implemented through the Information Highway

**only 20%**


of requests (209 out of over 1,000) for information transfers submitted by bodies to the Population Authority are managed in the designated system (Moed), which is supposed to manage the information transfer processes between bodies

<sup>6</sup> The Information Highway is a central infrastructure that provides a uniform, organization-wide solution based on the development of standard interfaces for the secure transfer of information between government ministries and public bodies.






## Audit Actions

 In 2021, the State Comptroller's Office audited the implementation of the Ask Once Policy (the Previous Report or Audit<sup>7</sup>). The primary issues addressed in the Previous Audit included the process of mapping government services, establishing objectives for minimizing the information and approvals necessary for the public to access services, developing a system for managing the operations of information transfer committees (the Moed system), and establishing the government Information Highway (the Information Highway or Highway).


From June to December 2023, the State Comptroller's Office conducted a focused follow-up audit on significant findings from the Previous Audit, including the implementation of the Ask Once Policy by National Digital Agency the and promoting the supporting infrastructures and the Moed system. It should be noted that this audit examined additional aspects not addressed by the Previous Audit, raised findings from these examinations, and included them in the follow-up report.

## Key Findings



 **Mapping and Validation of Services – the follow-up audit** raised that twelve bodies failed to validate their services, encompassing 480 services at the Ministry of Education and 129 at the Rabbinical Courts. Furthermore, despite a government resolution adopted eight years ago, the National Digital Agency has yet to establish a comprehensive policy for the mapping and validation of services, including updating and enhancing the service database. Consequently, the Agency lacks a complete and current situation report of all government services and the necessary information and approvals for their delivery.



 **Expanding the Mapped Bodies – the Previous Audit** recommended that the ICT Authority and Israel Digital assess the feasibility of incorporating additional public bodies that offer numerous services to the public, such as local authorities, hospitals, and HMOs, into the mapping process. **The follow-up audit found that this deficiency has not been rectified** and that despite the State Comptroller's earlier recommendations, the examination has not been conducted, and services provided by public bodies that are not government bodies have yet to be mapped and validated. This adversely affects the

<sup>7</sup> Annual Audit Report 72A (2021) "Ask Once Policy" to Improve the Governmental Digital Service to the Public".



efforts to enhance public service and mitigate the bureaucratic burden, deviating from the government's 2020 plan to expedite digital services for the public.

**📌 Government Ministries' Use of the Information Highway** – the Previous Audit raised that three bodies (the IDF, the Tax Authority, and the National Insurance Institute) required to implement the Information Highway for information sharing by April 2021 had not complied. **The follow-up audit found that this deficiency has not been rectified** and that these bodies are still not connected to the Information Highway, failing to adhere to the government's resolution, the State Comptroller's recommendations in the Previous Audit, and the ICT Authority's plan for connection to the Information Highway. **Additionally, the follow-up found** that three other bodies – namely, the Ministry of Defense, the Ministry of Energy and Infrastructure, and the Israel Antiquities Authority – have also not established connections to the Information Highway, contrary to the government resolution and ICT Authority deployment plans. **Moreover**, about eight years following the government's mandate for ministries and auxiliary units to utilize the government's technological infrastructure for information sharing (the Information Highway), this infrastructure has been employed for less than one-third of all services (1,178 out of 3,888). Consequently, for most services (70%), government ministries rely on local infrastructures, email, or require citizens to provide the necessary information independently. The insufficient utilization of the Information Highway undermines the intended benefits, hindering the enhancement of public service and the implementation of the Ask Once Policy, which minimizes the inconvenience for citizens due to repetitive information requests by multiple government bodies.

**📌 The Ministry of Defense's Use of the Information Highway** – it was found that the Ministry of Defense does not obtain various approvals from government ministries directly via the Information Highway; instead, it requests approvals from bereaved families and IDF-disabled members. The State Comptroller's Office has commented to the Ministry of Defense that, in its civilian operations, it must provide services to the public through the secure digital platform provided by the National Digital Agency, just like all other government ministries. There was an expectation that during the Iron Swords War, with an increase in bereaved families and disabled individuals, the Ministry would enhance its service delivery to these populations by utilizing the Information Highway and implementing the Ask Once Policy, thereby alleviating the need for these populations to obtain approvals and certifications from multiple ministries unnecessarily.

**📌 Implementation of the Ask Once Policy** – the Previous Audit raised a lack of a comprehensive and detailed situation report regarding implementing the Ask Once Policy within government ministries. It was recommended that the ICT Authority and Israel Digital establish specific targets at both the ministry and service levels, along with a multi-year timetable for progress, to ensure the achievement of the targets outlined in the government resolution. **The follow-up audit has found that this deficiency has not been rectified.** Eight years after the government resolution and four years after the Previous Audit, the National Digital Agency still lacks information or data concerning



the scope of government services implementing the Ask Once Policy and the potential services that could adopt this policy. Furthermore, the National Digital Agency does not possess mechanisms for monitoring the implementation of the Ask Once Policy within government ministries or supervising the matter. Additionally, no specific targets have been established at the ministry and service levels for integrating government services under the Information Highway or implementing the Ask Once Policy from 2021 to 2023. A multi-year timetable for progress has also not been set to ensure the achievement of the objectives established in government resolutions 1933 and 260, regarding the implementation of the Ask Once Policy and expanding digital services to the public. There is no process for monitoring and publicizing compliance with these resolutions.

### **Transfer of Information Between Bodies and the Implementation of a "Committee System" for Managing Information Transfer (Moed system)**

- **In the Previous Audit**, it was recommended that the ICT Authority annually submit a report to the government regarding the work of the committees for information transfer, including data on processing times for requests at each stage, particularly regarding significant bottlenecks and reasons for delays. **The follow-up audit found that this deficiency has not been rectified** and that since 2020, the National Digital Agency has not prepared or submitted any annual reports to the government. Furthermore, the steering committee, established under the government resolution to supervise the implementation of the resolution regarding information transfers between ministries to promote the ask once policy, did not convene at all in 2021–2023, effectively ceasing operations. This is despite the government's mandate for the steering committee, chaired by the Agency, to provide annual updates on the implementation status. The absence of steering committee meetings and lack of public information publication has undermined control over the implementation of the resolution. This lack of supervision is particularly evident in light of audit findings regarding using the Moed system and extended processing times for information transfers between ministries.
- **The Previous Audit** raised that only about 9% of all requests processed by committees for information transfers between public entities in 2019 were managed via the Moed system. **The follow-up audit found that this deficiency had not been rectified.** The National Digital Agency lacks data on the volume of information transfer requests not processed through the Moed system, indicating that many requests are not handled through said system. Specifically, it was found that in 2021–2023, only 209 requests were submitted to the Population Authority via the Moed system, representing about 20% of all information transfer requests submitted during that period.
- **The Follow-up audit** found that in 2018–2023, the average processing time for a request by the body holding the information was 277 days, exceeding the 60-day timeframe set in the government resolution. Thus, the processing time for information transfer requests extended four times longer than mandated. The



lengthy processing duration – about nine months or more from the submission of a request to its approval – impairs public service delivery, reflects inefficiency, imposes bureaucratic burdens, and waste of resources and managerial attention to the ongoing process. It should be noted that the extended processing time undermines the implementation of the Ask Once Policy based on information transfer between ministries.



#### **Transfer of Information Between Ministries During the "Iron Swords" War –**

**Firearms Licensing** negotiations between the Israel Defense Forces and the Ministry of National Security to develop an online interface for transferring data between the two bodies have been going on for years. However, as of April 2024, this interface had yet to be established, including through the Information Highway. Consequently, citizens applying for a firearms license must apply to the IDF for confirmation of military service (Form 830) concurrently with their license application. Upon receiving confirmation from the IDF, the applicant must then forward this confirmation to the Ministry of National Security. **The follow-up audit found** that due to the significant increase in firearms license applications following the onset of the war, the Ministry of National Security reached out to the IDF in October 2023 to expedite the establishment of the interface. In November and December 2023, official requests were submitted to obtain the necessary information for the committee's decision on data transfer, adhering to privacy protection regulations. It was not until April 2024, six months after the war began, that the IDF's online interface for firearms licensing with the Ministry of National Security was finally launched. This delay occurred despite a substantial backlog, which reached about 240,000 unprocessed applications by December 2023, highlighting the urgent need for efficient data transfer from the IDF to the Ministry of National Security to facilitate timely reviews of firearms license applications during the conflict. This situation underscores the detrimental effects of non-compliance with government resolutions regarding utilizing the Information Highway and implementing the Ask Once Policy.



**Mapping and Validation of Services – the Previous Audit** raised that only 933 (26%) of the 3,545 public services mapped had undergone the necessary analysis and validation of service characteristics, including required references and involved bodies, by the service-providing ministries in collaboration with the National Digital Agency. The lack of analysis and validation impedes the identification of services suitable for implementing the Ask Once Policy or those that effectively implement it and achieve significant bureaucratic alleviation, making it challenging to engage with the relevant ministries to enforce government resolutions. Moreover, it was recommended that timetables and targets for progress in creating a service database and validating it with ministries be established, adherence must be monitored and reported to the government, and ways for timely and effective information updates and improvements must be considered. **The follow-up audit found that the deficiency has been largely**



**rectified**, with 2,742 out of 3,888 mapped services (70%) validated by the National Digital Agency in collaboration with government ministries.

**Transfer of Information Between Bodies – the Previous Audit** recommended the development of an online form facilitating efficient interaction within the Moed system and external public bodies. **The follow-up audit found that the recommendation was implemented.** The National Digital Agency now provides external public bodies, which are not connected to the Moed system, with an online form linked to the Moed system.

## Key Recommendations

- 💡 The National Digital Agency should develop a comprehensive work plan for advancing the Ask Once Policy, including timelines mandating all government ministries, auxiliary units, and public bodies that have not yet mapped and validated their services or those not connected to the government Information Highway, to establish a suitable infrastructure to implement the Ask Once Policy. Should the National Digital Agency lack sufficient authority to promote necessary actions by these bodies as stipulated in the government resolution, it should expand its directive authority through a government resolution or other designated means. Furthermore, the Agency should consider anchoring all timetables in a binding government resolution.
- 💡 The Ministry of Education, the Ministry of Environmental Protection, the Rabbinical Courts, the Israel Tax Authority, the Employment Service, the Ministry of Interior, and the Ministry of Culture and Sports, in collaboration with the National Digital Agency, should map and validate the services they provide to the public.
- 💡 The IDF, the Tax Authority, the National Insurance Institute, the Ministry of Defense, Energy and Infrastructure, the Antiquities Authority, and the Central Bureau of Statistics should connect to the Information Highway. They should facilitate information transfers to and from them via the Highway, leveraging its advantages to realize the Ask Once Policy in public service provision, particularly regarding life events specified in government resolutions: birth, relocation, job transitions, disability, nursing care needs, death, business initiation, and commercial import.
- 💡 The Ministry of Defense should promptly implement the government resolution and adhere to the State Comptroller's recommendations in the Previous Report regarding its connection to the Information Highway, thereby ensuring compliance with the Ask Once Policy in service delivery.
- 💡 The National Digital Agency should ensure that all government bodies that have yet to fulfill their obligations comply with government resolution regarding connection to and utilization of the Information Highway and update the Information Highway deployment plan



accordingly. This plan must include mandatory timelines for connecting the relevant bodies to the Information Highway in alignment with the government resolution. Moreover, the Agency should define success metrics and supervise their implementation. Additionally, all relevant ministries and public bodies should connect to the Information Highway and deliver their services accordingly. Government ministries' success indicators and compliance with these objectives should be reported to the government and the public as part of the Agency's annual report.



The head of the National Digital Agency should reinstate the steering committee on information transfers and convene it to supervise the operations of government ministries and public bodies in achieving the Ask Once Policy goal while also monitoring failures in implementing the stated policy. Thus, enhancing governmental service to the public and alleviating bureaucratic burdens. Moreover, the committee should report to the government on the execution of the resolution, particularly concerning the actual timelines for information transfers between bodies. It should also clarify to all public bodies their responsibility to manage the approval processes for information transfers and to execute them effectively and efficiently through the infrastructure provided, including the Information Highway and the Moed system, thereby streamlining and improving public service.



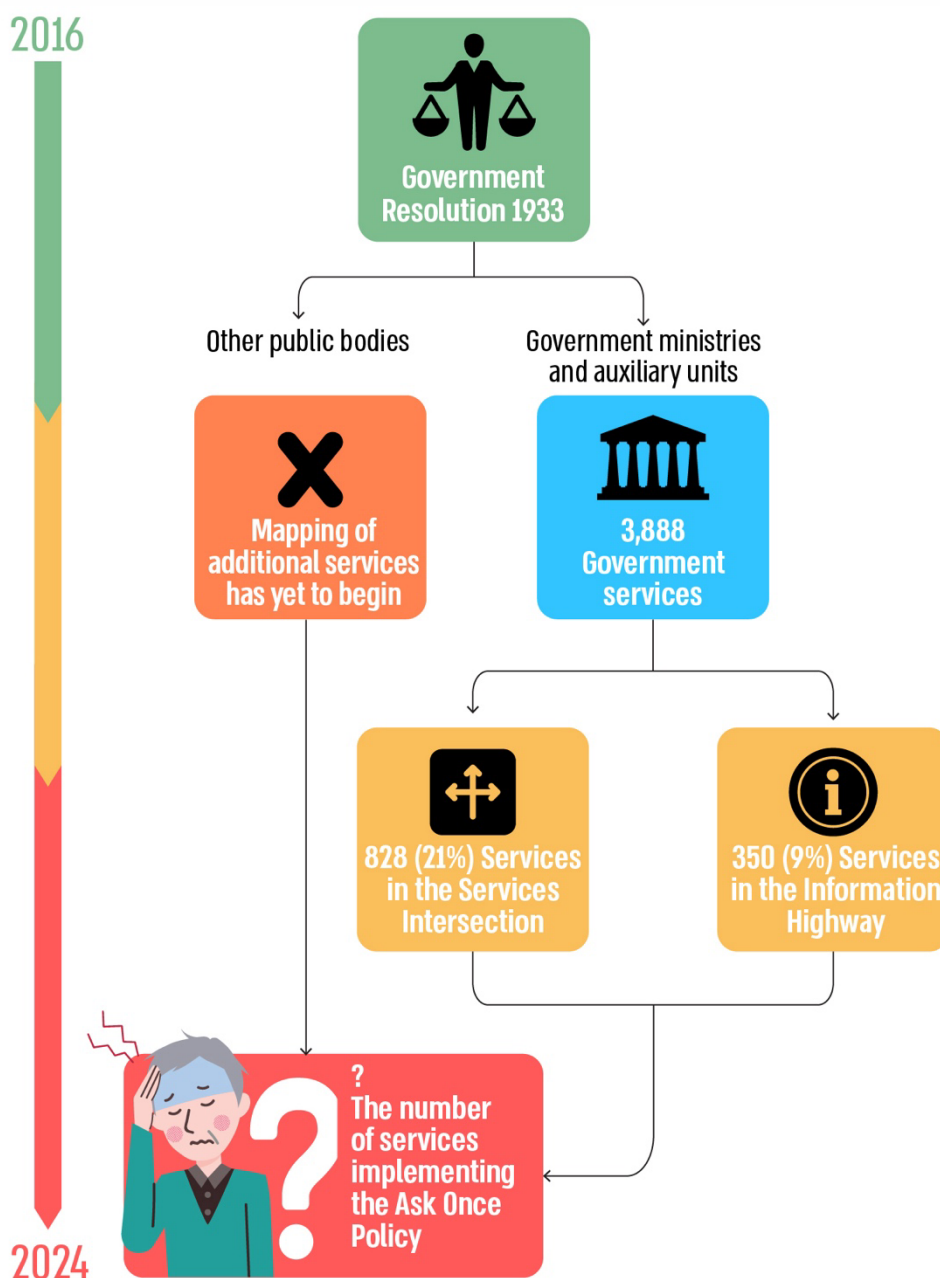
The Ministry of Justice should finalize the work of the inter-ministerial team focused on enhancing the information transfer domain, instituting significant reforms to the overall process in line with government resolutions, and ensuring substantial reductions in both approval timelines and information transfer durations among bodies. The National Digital Agency should improve the information transfer processes within the ministerial committees, involving automation and digital management processes in the new Cheeta system<sup>8</sup>. This reduces the processing time from application submission to final decision to under 60 days, as mandated by the government resolution.

---

<sup>8</sup> A new information system established by the National Digital Agency to manage information transfer procedures between ministries.



## Number of Services Implementing the Ask Once Policy, Eight Years After the Government's Resolution



According to data from the National Digital Agency, processed by the Office of the State Comptroller.



---

---

## Summary

To reduce the bureaucratic burden and enhance public service, the government decided to implement the Ask Once Policy in 2016. This policy stipulates that if a public body requires information to provide a service, it should not request this information from the citizen or business if another public body already possesses it. Instead, the information should be directly obtained from the holding body. In 2020, the government accelerated the adoption of digital services by advancing the Ask Once Policy. The Iron Swords War demonstrated and even highlighted the importance of providing digital services to the public while implementing the Ask Once Policy.

In 2021, the State Comptroller's Office published the Previous Report, which showed significant progress was still needed before achieving the 2021 mandate prohibiting ministries from requesting certificates from the public that are available through other ministries. Four years after the resolution, a clear picture of the implementation status of the Ask Once Policy was still lacking, hindering goal-setting for ongoing policy enforcement, including establishing milestones and monitoring.

The follow-up audit, conducted eight years after the initial government resolution, examined the rectification of the key deficiencies found in the Previous Audit and raised significant progress in the preliminary actions required to implement the Ask Once Policy, particularly concerning the mapping of government services provided to the public and the analysis of their characteristics. However, most deficiencies noted in the Previous Report were not addressed. The utilization of the Information Highway – a technological infrastructure designed to facilitate secure, cross-ministerial information transfer between all government ministries – currently encompasses only 9% of government services. Additionally, the objectives set in government resolutions are not being met. The National Digital Agency lacks data concerning the scope of actual and potential services for implementing the Ask Once Policy, and it fails to submit timely reports on compliance with governmental resolutions to the government. Additionally, the inter-ministerial steering committee established to monitor the implementation of these resolutions has not convened.

Efficient inter-ministerial information transfer is critical for the Ask Once Policy. The follow-up findings indicate that ministries are not adhering to government resolutions or the guidelines of the National Digital Agency. Processing times for inter-ministerial information transfer exceeded designated limits by over 300%, with an average transfer time of about nine months, compared to the 60-day target. This illustrates a low level of commitment from ministries and auxiliary units to fulfill government resolutions.

During the Iron Swords War, in light of the excessive scope of about 240,000 new firearm license applications pending with the Ministry of National Security as of December 2023, a request for information transfer via an online interface was made to the IDF. However, this





interface was not operational until April 2024, nearly six months following the onset of the war, despite the urgent need for rapid information exchange.

The government plan established in 2016 has yet to be effectively implemented after eight years, and the completion of the process does not seem foreseeable. The fundamental issue appears to be the limitations of the National Digital Agency's capabilities to enforce the plan, as its interactions with government bodies do not compel government ministries to take actual action. This deficiency, combined with a lack of commitment from government and public bodies to adhere to the resolution and the National Digital Agency's directives, has resulted in inadequate execution of the Ask Once Policy.

To expedite policy implementation, the National Digital Agency should adopt a comprehensive strategic approach addressing all contributory factors, requiring a commitment from all government ministries and auxiliary units. Including mapping and validating public services, connecting ministries to the Information Highway, establishing supporting portals, and improving inter-ministerial information transfer processes, including coordination through the Moed system. It is recommended that local government and the health sector be included in advancing government policy. Addressing the deficiencies in the Previous Audit will enhance public service delivery and governmental efficiency. Should the National Digital Agency require additional authority to implement these measures, it must engage with the government to secure such powers.

The National Digital Agency should transparently report the extent of implementation of the Ask Once Policy concerning information transfers in its annual reports. Without significant progress, the National Digital Agency should bring the matter to the government, advocating for updated resolutions that impose binding timelines on government ministries and public bodies.



The Minister of Economy, responsible for the National Digital Agency, should supervise the enforcement of government resolutions and periodically report to the government on the policy progress. The inter-ministerial team, led by the Ministry of Justice, should finalize discussions and present the government with a proposal to eliminate barriers and promote effective and rapid information transfer between ministries and public bodies, thus supporting improved public service and reduced bureaucracy.




### The Rectification Extent of the Key Deficiencies Noted in the Previous Report

The Audit Chapter	The Audited Body	The Deficiency in the Previous Audit Report	The Rectification Extent of the Deficiency Noted in the Follow-up Audit			
			Not Rectified	Slightly Rectified	Significantly Rectified	Fully Rectified
Transfer of information between bodies and the Moed system	ICT Authority	The ICT Authority should develop an online form for an efficient working interface on the Moed system with external public bodies.				
Mapping and validation of services provided to the public	ICT Authority, Israel Digital, government ministries, and auxiliary units	Government ministries and auxiliary units, in collaboration with the National Digital Agency, validated only about 26% of all services mapped (933 out of 3,545). Without full validation of the mapped services, the ICT Authority and Israel Digital did not have a complete and reliable situation report of each ministry's total services to the public, the information and authorizations required to receive each service, and the originating body issuing each authorization.				




The Audit Chapter	The Audited Body	The Deficiency in the Previous Audit Report	The Rectification Extent of the Deficiency Noted in the Follow-up Audit			
			Not Rectified	Slightly Rectified	Significantly Rectified	Fully Rectified
Mapping and validation of services provided to the public	ICT Authority and Israel Digital	It was recommended that the ICT Authority and Israel Digital consider incorporating additional public bodies that provide many services to the public, such as local authorities, hospitals, and HMOs, into the mapping to consider the implementation of the Ask Once Policy.				
Government ministries' use of the Information Highway	Tax Authority, National Insurance Institute, Ministry of Defense	Three bodies that Government Resolution 260 of 2020 required to externalize information on the Information Avenue by April 2021 have not yet implemented the system – the Tax Authority, the National Insurance Institute, and the Ministry of Defense.				




The Audit Chapter	The Audited Body	The Deficiency in the Previous Audit Report	The Rectification Extent of the Deficiency Noted in the Follow-up Audit			
			Not Rectified	Slightly Rectified	Significantly Rectified	Fully Rectified
Implementation of the Ask Once Policy	The ICT Authority	In August 2020, the ICT Authority did not have a complete and detailed picture of the rate of implementation of the Ask Once Policy in the ministries at all levels, and it was also impossible to maintain an optimal process of setting goals for implementing the policy, including setting milestones for progress and monitoring their implementation.				



The Audit Chapter	The Audited Body	The Deficiency in the Previous Audit Report	The Rectification Extent of the Deficiency Noted in the Follow-up Audit			
			Not Rectified	Slightly Rectified	Significantly Rectified	Fully Rectified
Transfer of information between entities and the Moed system	The ICT Authority	It was recommended that the annual report that the ICT Authority submits to the government regarding the work of the committees include data regarding the processing times for requests at each stage, significant bottlenecks in the request approval process, and the reasons for delays. Thus, a complete situation report of the information transfer process on both the requesting and the holding side of the information will be provided, as well as the stages in the process that require improvement.				



The Audit Chapter	The Audited Body	The Deficiency in the Previous Audit Report	The Rectification Extent of the Deficiency Noted in the Follow-up Audit			
			Not Rectified	Slightly Rectified	Significantly Rectified	Fully Rectified
Transfer of information between entities and the Moed system	The ICT Authority and relevant government ministries	Only 9% of all requests processed by committees for information transfers between public bodies in 2019 were processed through the Moed system. The ICT Authority and bodies not yet connected to the Moed system should do so.				



Report of the State Comptroller of Israel – Cyber and  
Information Systems | November 2024

Israel Postal Company

---

# **Information Systems at the Israel Postal Company and the Postal Bank**







## Information Systems at the Israel Postal Company and the Postal Bank

### Background

The Israel Postal Company is a government company wholly owned by the State of Israel, which provides postal services and operates banking services through its subsidiary – the Postal Bank. As of the end of 2023, the Israel Postal Company and the Israel Postal Bank operate 400 postal units, 650 delivery centers, and about 60 regional postal centers. In 2023, about 11.9 million customers received services from the Company and the Bank.

The Postal Company offers diverse services, including domestic postal services, shipping documents and goods between Israel and abroad, and a network of courier centers distributing for business and private customers across the country.

The Postal Bank serves business customers, government bodies, and the general public. It is government-owned and operates under the supervision of the Ministry of Communications, similar to the Israel Postal Company. Services are offered through about 400 postal branches, including banking teller services. The Postal Bank manages around 510,000 bank accounts, with total deposits of about NIS 4.7 billion. It carries out about 22 million transactions with casual customers annually, and the total number of its customers is about one million.

The Postal Company and Postal Bank utilize various information systems, encompassing operational systems for export and customs, digital services, courier services, banking and retail, headquarters operations, infrastructure and information security, operation and telephony systems.

In April 2023, a cyber-attack on the postal information systems was identified. An examination conducted by the Information Systems Division's information and cyber security teams on April 2, 2023, raised suspicious activity within the postal information systems. On April 5, 2023, an incident response<sup>1</sup> (IR) team from an external cybersecurity firm was engaged. As a precaution, the Company disconnected the postal systems from the Internet. The external firm discovered indicators of unauthorized activity within the organization's systems dating back to July 2022. Despite their efforts, the external company could not identify the attacker, who successfully extracted the user and password database. Consequently, numerous services were rendered inactive, including online payments, vehicle ownership transfers,

1 Incident response to cyber incidents team.



payments to the execution offices, and transfers to HMOs, along with delays in releasing items from abroad. As the work of the external team progressed, services were gradually restored.

### Key Figures

**NIS 124  
million**

annual average operating and investment expenses of the Information Systems Division in 2019–2022

**55**

information systems at the Israel Postal Company. The Postal Bank has 16 additional information systems

**48.75%**

the decrease rate in the planned investment budget in the Information Systems Division from NIS 64.2 million in 2019 to NIS 32.9 million in 2022

**64%**

inquiries rate regarding hardware failures out of the total failures inquiries that Shut down end stations in postal units

**683**

computers were replaced or upgraded out of the 1,850 that required replacing or upgrading to WIN 10

**85**

of System C<sup>2</sup> permission holders (3% of all permission holders) are not defined in the Human Resources system as active employees in the Company as of January 2024

**780**

of active permission holders in the network's<sup>3</sup> central management system (13% of all permission holders) are employees who are not included in the list of active employees in the Company's Human Resources system

**449**


out of 780 active permission holders who are not listed as "active" in the Human Resources system have not logged on to the network's central management system since the beginning of 2024

2 The central system for managing teller processes also serves as the Israel Post cash register for all financial transactions carried out in branches and offices.

3 A dedicated set of tools used for centralized management of computer networks in organizations.



## Audit Actions

 From June 2023 to March 2024, the State Comptroller's Office Audited the Israel Postal Company and the Postal Bank information systems. The audit was performed at both the Postal Company and the Postal Bank. The audit examined the management and control user permissions at the Postal Company. Additional examinations were conducted at the Ministry of Communications.

## Key Findings



**Connecting the Postal Company's Security Operations Center (SOC) to the Ministry of Communications' Sectoral SOC** – a critical component within the system for securing organizational data and resources is the Security Operations Center (SOC). This center among other roles, monitors unusual activities, assesses potential threats, and provides insights based on investigations following incidents. The Postal Company operates its SOC under the supervision of the Information Systems Division and procures SOC services from a private entity. The audit raised that during 2022–2023, the Ministry of Communications' sectoral unit, which operates a sectoral SOC funded by both the Ministry of Communications and the National Cyber Directorate, made multiple inquiries to the Postal Company regarding connectivity to the Ministry's SOC. However, the Postal Company had not established this connection as of the audit end date. Consequently, the Company is not using the advantages inherent in connecting to the Ministry of Communications SOC, including enhanced external supervision during cyber incidents.



**Annual and Multi-Annual Work Plans in the Information Systems** – despite a substantial budget for the Information Systems Division at the Postal Company, from about NIS 102 million to NIS 136 million, 17.2% to 19.6% of the Company's total budget (about NIS 102 million out of a total budget of about NIS 592 million in 2022 and about NIS 136 million out of a total budget of about NIS 693 million in 2020), no established procedure exists for managing work plans. Furthermore, in 2019–2023, no multi-annual work plan for information systems was developed. The formulation process for the work plan, as of 2023, does not incorporate departmental alternatives and predominantly relies on a fixed budget. The execution of the work plan lacks monitoring, inhibiting the management's ability to ascertain its status or any adjustments made. Additionally, tracking budget reallocations across tasks is unfeasible, and even the Management of the Information Systems Department lacks transparency regarding allocating working hours per task. It should be noted that in 2024, the Company implemented specialized software for team and project management.



**Malfunctions in Information Systems at the Postal Company and the Postal Bank** – in 2018, the Information Systems Department presented the need to replace outdated computing equipment in the end stations due to numerous hardware malfunctions. According to the Company's data, from April 1, 2022, to July 21, 2023, system users submitted 46,349 inquiries classified as hardware malfunctions. These inquiries represent the largest category, at about 35% of total inquiries. About 64% of inquiries related to faults resulting in the shutdown of end stations identified hardware issues of 3,306 inquiries out of 5,178 examined. Additionally, about 32% of malfunctions that led to complete postal unit shutdowns during the examined period were hardware-related, of 525 malfunctions out of 1,618 examined. Notably, roughly 80% of all hardware malfunctions lead to end station shutdowns, and about 92% of such malfunctions result in postal unit shutdowns related to computerized equipment, some of which had already been identified for replacement in 2018. This data underscores the detrimental impact of outdated hardware on the operational efficacy of postal units and, consequently, on the quality of service provided to customers.

**Project for the Replacement of Outdated Computer Equipment at the Postal Company and Postal Bank** – the equipment replacement project<sup>4</sup> was approved within the work plans for 2019–2023. Concurrently, the upgrade to Windows 10 operating systems commenced. This project has been classified as strategic since 2019. However, the Postal Company only began acquiring new computer equipment at the beginning of 2022. As of the audit end date, over four years after the necessity for replacement emerged, numerous malfunctions stem from the delayed equipment replacement, underscoring the urgent need for new equipment. By March 2024, the Company had replaced and upgraded only 683 computers (about 37%) of the required 1,850 computers to Windows 10. By contrast, only 196 (about 56%) of the 350 plasma computers requiring upgrade were upgraded, and only 136 (about 68%) of the 200 queue management systems needing upgrade were completed. The audit also found that annual depreciation on computers and equipment is marginally lower than the purchase values in most years. Total expenditures on computers and peripheral equipment from 2019 to 2022 were NIS 39.8 million, while the total annual depreciation for the same period was NIS 37.4 million (around 94%). These figures indicate that the Company's investments in software and equipment purchases only slightly surpass the depreciation of prior investments. In 2022, investment in software and peripheral equipment purchasing fell below the depreciation of previous years' investments. Hence, the Company maintains the status quo without prioritizing continuous improvement in its information systems.

**Computerized Queue Management System** – since 2007, the Postal Company and Postal Bank have implemented queue management systems in select postal units using off-the-shelf software. The audit raised that the current system does not facilitate

<sup>4</sup> Computers, printers, computerized queue management stations, computer monitors, and other hardware equipment.



customers' input of information regarding the services for which they have reserved a queue<sup>5</sup>, nor does it allocate sufficient time based on customer needs. For example, the time required for a customer to open a bank account at the Postal Bank vastly exceeds that allocated for someone collecting a postal package. This discrepancy can lead to excessive wait times at Postal Bank branches, resulting in delayed service. Furthermore, the system cannot log the specific actions customers intend to undertake. Early identification of such actions could inform customers so they are better prepared with the necessary documentation or preparations required for the service. Although customers can independently cancel their queue, the system fails to send reminders to ensure their attendance or cancellation at the designated time. The misalignment between the queue management system and the Company's operational nature and requirements hampers effective queue management, adversely impacting customer service.

**Multiple Systems and No Interface Among Them** – as of the audit end date, 55 information systems, some of them divided into subsystems, were operational within the Postal Company, with the Postal Bank utilizing an additional 16 systems, some of them are divided into subsystems. These systems are sourced from over 20 different suppliers and employ various technologies. The existence of multiple systems without effective interfaces complicates system integration, diminishes data uniformity, and obstructs process management. This lack of integration creates challenges in synchronizing data across systems, potentially resulting in errors. Consequently, the Company invests in human resources or developing compensatory manual processes to establish system compatibility. For instance, the human resources information system lacks a computerized interface with the Bank's mainframe computer system<sup>6</sup>. When the need arises to revoke an employee's permissions<sup>7</sup> in the mainframe computer system, manual procedures are required: an email is sent from the Human Resources Department to the relevant parties in the mainframe computer system requesting permission revocation. Additionally, a monthly compensatory control process generates an anomaly report for employees who have retired or resigned but remain linked to the mainframe computer system, requiring a manual review of these anomalies. The unique identifiers in the Human Resources Department's information system differ from those in the mainframe computer system. Due to discrepancies in employee registration across both systems, the Company has created a manual conversion table to align employee ID numbers with usernames in the Bank's systems, which must be updated manually to address inconsistencies in data.

**Periodic Review of Permissions at the Postal Company** – the Postal Company conducts a manual review of permissions for 17 core systems biannually, specifically in January and August. However, permission reviews are not performed for the remaining


<sup>5</sup> Other than vehicle ownership transfers.


<sup>6</sup> A mainframe computer used to run many applications simultaneously, using large-scale data processing.


<sup>7</sup> Due to leaving or retirement.



systems, as mandated by the User and Authorization Procedure. Furthermore, there is no process to document anomalies identified during these reviews, which could assist in pinpointing systems or departments that frequently encounter numerous anomalies, allowing for timely responses. Additionally, no computerized control mechanism is in place to evaluate the alignment of permissions with the permission holders. For instance, when an employee changes positions within the department, the necessary adjustments to their assigned permissions may go unrecognized by the business manager conducting the survey.

 **Review of Permissions in System C at the Postal Company** – the audit found that, as of January 2024, 85 permission holders in System C (constituting 3% of all permission holders in this system) are not classified as "active" in the human resources system. This indicates that the permissions of former employees have not been terminated, or their status was not updated in the human resources system. Despite compensatory automatic controls, errors were detected in the computerized control process, as the audit findings confirmed that 79 employees with active permissions were not identified by the automatic control while also not being marked as "active" in the human resources systems.

 **Permissions in the Central Network Management System at the Postal Company** – the audit found that, as of December 2023, 780 (about 13%) of the active permission holders in the central network management system are employees not recognized as "active" in the Company's human resources system. Among these, 449 (about 58%) have not accessed the central network management system since the onset of 2024. There is a lack of information regarding the last login date for 196 (about 25%) of the permission holders, while it is known that 135 (about 17%) had their last login in 2024. It can be concluded that employees who have not logged in since 2023 and those lacking last login data are likely former employees whose permissions remain active. Moreover, employees who have recently logged-in in 2024, presumably active, still are not listed as "active" in the HR system. Notably, 70 of the 80 employees with active permissions in the audit sample<sup>8</sup> do not work at the Postal Company. Six employees who departed as early as 2020 had yet to have their permissions revoked at the time of sampling, over three years post-departure. The permissions of another employee who left in 2021 and three others who exited in 2023 remain unrevoked. Not revoking permissions for employees who are not "active" could potentially lead to unauthorized access and misuse of valid permissions to the detriment of the Company.

 **Examination of Permissions on the Mainframe Computer at the Postal Bank** – an examination of permissions on the mainframe computer at the Postal Bank raised that 35 users, about 2% of the 1,794 active permissions, belong to employees not classified as active within the human resources systems. While most users must log in to the

<sup>8</sup> 80 out of 780 active permission holders in the network's central management system are not included in the list of active employees in the Company's human resources system.



central management system before accessing the mainframe computer, these findings pose significant concerns regarding the critical importance of information security at the Bank. Granting active permissions to individuals not employed by the Bank raises the potential risk of compromising information security.

**🔴 Examination of Permissions on the Central Management System of the Postal Bank Network** – a review of the central management system permissions indicated that 67 users with active permissions are either not marked as "active" in the human resources systems or cannot be located. Upon further investigation, it was found that 58 of them are external information systems personnel. An examination of the remaining nine user permissions found that permissions for three employees on maternity leave were not revoked despite the procedural requirement to revoke permissions for employees absent for over one calendar month. One employee, who left the Bank on June 30, 2023, returned to work but remains classified as inactive in the Human Resources Department. Another individual who left the Bank retains permissions, and three active employees are not recognized as such in the human resources systems despite being listed in the alignment table. Moreover, others continue to utilize the username of a former employee. The failure to revoke permissions for individuals deemed inactive within sensitive banking systems compromises the Bank's information security and increases the risk of unauthorized access to its systems.






**🔴 Collection Process for Balances from Post Offices** – daily operations involve Company drivers collecting physical references for banking transactions from end stations (balances<sup>9</sup>), placing them in bags, and transferring these to the Postal Bank headquarters at the sorting center in Modi'in. The Company has not met its target of 85% of balances arriving the next day; Currently, only 70% arrive within two days. Control and monitoring of balance arrivals at Postal Bank headquarters are inadequate, with no daily supervision of balances not collected from the preceding business day, preventing confirmation of their arrival at the Postal Company until the monthly audit. Furthermore, no follow-up monitoring is conducted after this inspection. Balances have been left unattended in the sorting hall for extended periods, exposing them to the risk of theft or unauthorized access, which has persisted for years.

9 These balances include, among other things, checks, vouchers, bank forms, and checks for deposit.



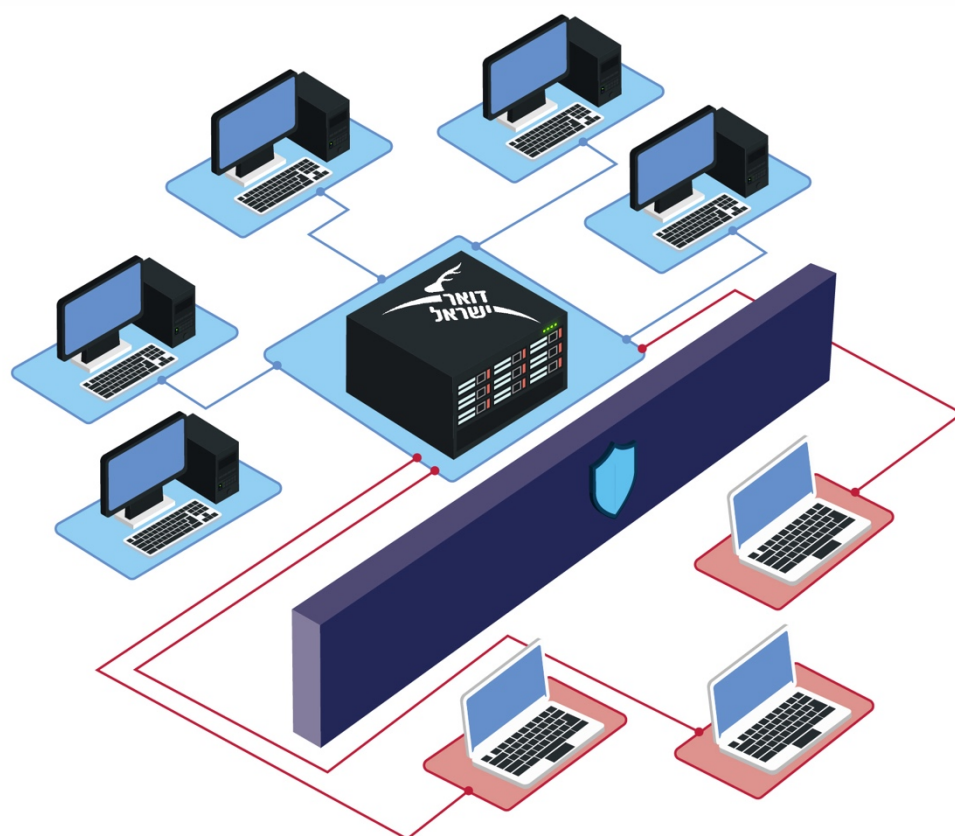
---

## Key Recommendations

-  The Company should regulate annual and multi-annual work plan issuance and ensure its implementation. This includes evaluating alternatives, monitoring the execution of the work plan, and providing the management of the Information Systems Division with an updated overview of ongoing tasks, their costs, and their scope.
-  The Company should promptly complete the project to replace outdated equipment in its units to mitigate risks and enhance customer service.
-  The Company should implement the 2021 master plan's recommendations to prevent duplication and unnecessary activities by formulating and developing standardized operational processes that leverage digital and information technologies.
-  The Company should conduct routine permission checks within the network's central management system to minimize risks associated with granting access to unauthorized employees and to facilitate permission management across multiple systems. Furthermore, the Company should review the permission-checking process in System C and all other systems under evaluation to identify failures in recognizing inactive employees, particularly concerning the review of manual authorizations. Additionally, it is necessary to locate all employees classified as inactive users who possess permissions in various systems and comprehensively examine the control mechanisms governing user permissions, making improvements based on the findings.
-  The Company should enhance control measures at the Postal Bank, regularly reconciling the data of authorized individuals with that from the Human Resources Department. Furthermore, it should develop automated processes for revoking permissions within the Bank's systems and supervise these permissions.



## Audit Findings in Examining Permissions in the Central Network Management System at the Postal Company



# 780

Of the active permission holders in the networks central management system are not included in the list of "active" company employees



---

## Summary

The Postal Company operates 55 information systems, several of which are divided into subsystems, while the Postal Bank utilizes an additional 16 systems, some comprising subsystems. These systems are supported by over 20 suppliers and based on various technologies.

This report raised deficiencies in the information and security systems within the Postal Company and the Postal Bank. Inadequate management of the employee permission revocation process and in controlling this process; Reliance on outdated computer equipment that adversely affects service delivery and jeopardizes information security; Absence of a multi-year strategic plan for the Information Systems Division; Lack of supervision in the execution of work plans; And multiple systems that hinder information transfer, necessitating manual procedures and resource allocation to mitigate these challenges.

The Information Systems Department at the Postal Company should develop a structured action plan that focuses on advancing information systems with a forward-thinking vision, modernization of outdated systems, and optimization of existing systems and their integration, all while ensuring robust cyber protection and minimizing risks associated with unauthorized access.

As part of improving information security, particularly given the recent cyber incident in April 2023, the company should improve control permission management. The Company must address the deficiencies noted in the audit and devise ways to rectify them promptly.



Report of the State Comptroller of Israel – Cyber and  
Information Systems | November 2024

The National Insurance Institute

---

# **Information Security and Cyber Protection at the National Insurance Institute**





## Information Security and Cyber Protection at the National Insurance Institute

### Background

The National Insurance Institute (NII) maintains an extensive database containing information from numerous organizations and government bodies, amounting to many terabytes (TB) in size. This database grows at about 10% annually, and it encompasses information on all residents of the State of Israel from birth until death. NII's databases are mandated to uphold a high level of security under the Privacy Protection (Information Security) Regulations, 2017<sup>1</sup>.

In July 2023, a Supreme Steering Committee for the Protection of Computer Systems in Israel<sup>2</sup> decided that the NII meets the required criteria and should be guided as a Critical Cyber Infrastructure body (CCI). Consequently, the Committee recommended the inclusion of the NII in the Fifth Schedule to the Regulation of Security in Public Bodies Law, 1998, to be guided by the National Cyber Directorate (NCD) under this law. As of April 2024, the audit completion date, approval has not yet been received for adding the NII in the Fifth Schedule of the law above. In alignment with its transformation into a CCI body, the NII has initiated proactive measures to enhance its protective measures, following the designated methodology for CCI bodies.

As of February 2024, the NII is subjected to tens of thousands of cyberattack attempts daily. A cyber incident affecting the NII could significantly harm the privacy of millions of citizens and residents receiving services from the NII, potentially disrupting operations and impairing the ability to disburse benefits (old age, disability, subsistence, unemployment, reserve benefits). A pertinent example of a severe information security incident at the NII, as defined in the Regulations, occurred in February 2022 when an identity theft event was reported, exposing the personal information of 2,000 citizens to unauthorized access.

1 Regulation 1, the Second Schedule and Fifth Schedule to the Information Security Regulations.

2 Government Resolution B/84 of 2002, which determined that a supreme steering committee should be established for the protection of computer systems in the State of Israel, whose role would be to examine which bodies would be defined as "essential" and therefore in need of cyber protection. Responsibility for this protection was assigned to the Israel Security Agency (ISA). In 2016, as part of an amendment to the Regulation of Security in Public Bodies Law, 1998, this responsibility was transferred from ISA to the National Cyber Directorate.



## Key Figures

### 10 years

the NII's cyber protection policy has not been updated, though significant changes have occurred since then. 50% of the procedures that, according to the Protection of Privacy Regulations (Data Security), are required to be included in every organization's information security procedure do not exist at the NII

### tens of thousands

the number of alerts on cyber-attacks on the NII per day that require investigation by a single analyst working at the NII Security Operations Center (SOC)

### over 2 years

the time during which the Cyber Steering Committee headed by the CEO did not convene – from the beginning of 2022 to January 2024

### 0

penetration tests were conducted on the central system of the NII

### 87%


of the Information Security Regulations are only partially implemented in the NII. No periodic audits are conducted to ensure compliance with regulations

### numerous bodies

receive information from the NII through information-sharing systems in which information security gaps were discovered




## Audit Actions


 From July 2023 to April 2024, the State Comptroller's Office audited information security and cyber protection at the National Insurance Institute (NII), focusing on compliance with the Information Security Regulations. The audit addressed several key areas, including cyber protection policies and procedures, risk management, information transfer from the NII to external entities, logical and physical protection, business continuity, response to cyber incidents, and supply chain management. The audit was performed at the NII, the Prime Minister's Office – the National Cyber Directorate, and the Ministry of Justice – the Privacy Protection Authority.


The Knesset State Audit Committee sub-committee decided not to submit data from this chapter before the Knesset to protect the state's security under Section 17(a) of the State Comptroller's Law, 1958 [Consolidated Version].

## Key Findings




 **Information Security and Cyber Protection Policy** – the NII has not updated its information security and cyber protection policy for nearly a decade, since 2014, despite significant changes in the risk landscape. This is inconsistent with its policy, requiring annual discussions and approvals of the information security policy. At the time of the audit, the policy document had been updated to draft status and approved in March 2024 by the Acting CEO of the NII; However, discussions have not yet been held by the Information Security Steering Committee as required by the policy document. Additionally, the policy document lacks explicit references to critical issues outlined by recognized standards, such as asset management, classification, and compliance controls with the Information Security Regulations.


 **Information Security Procedures** – the NII information security procedures inadequately address 6 of the 12 issues (50%) mandated by the Information Security Regulations that should be included within the information security procedural framework. Regarding 4 of the 12 issues (33%), existing procedures had not been updated in a decade, and in respect of 2 issues (17%), the most recent update dates are unspecified.


 **The Cyber Protection Steering Committee** – the Cyber Protection Steering Committee, led by the CEO, did not convene from early 2022 until January 2024, contrary to NII policy requiring biannual meetings. This lack of meetings resulted in the absence of a governing body to approve the cyber protection policy, endorse annual work plans,




monitor implementation, or present the cyber protection status, including gaps, significant events, and threats, to the organization's leadership. Furthermore, during the first committee meeting in January 2024, the cyber protection status was not presented to the NII's Acting CEO, the draft policy was not approved, and other essential topics defined in the committee's appointment letter were not discussed.

 **Risk Management** – the NII does not maintain a comprehensive inventory of all assets and business processes, nor does it classify them based on their level of importance to the organization, as mandated by the Information Security Regulations and industry standards, including the norms included in the protection doctrine<sup>3</sup>. The NII has identified a limited number of essential systems, mapping about one-third of those deemed most critical for examination in the survey. An ineffective risk management process lacking comprehensive asset mapping raises concerns that the risk management will not optimally reflect the main risks to which the organization is exposed, indicating that resources and actions to mitigate risks may not align adequately with the actual risk levels associated with the organization's assets. Additionally, the NII does not conduct risk surveys for its databases every 18 months, as required for organizations managing databases subject to high-security standards.

 **Penetration Tests** – the NII does not perform penetration tests on its databases under the Information Security Regulations and its internal policy document. As a result, about 7% of tests conducted relate to systems linked to the central system of all NII databases. Additionally, the NII does not monitor rectifying identified vulnerabilities, leading to persistent high-severity deficiencies that remain unresolved and expose the NII to potential risks. Penetration tests are also not executed on the central system, and there is a noted deficiency in knowledge and resources concerning implementing such tests within the NII and the NCD.

 **Logical Protection** – deficiencies were found across multiple domains in the NII logical protection.

 **Identifying and Handling Cyber Incidents** – deficiencies were found in the NII's capability to identify and manage cyber incidents. The NII does not have dedicated crisis management teams, including an incident response team (IR) and a digital forensic and incident response team (DFIR). A management team for cyber incident supervision was established at the end of January 2024 but has not yet convened, received training, or participated in drills. Additionally, gaps were found in the operations of the SOC, where the staffing team has not undergone specialized training. The SOC is supervised by the Infrastructure Division instead of the Information Security Division, creating a disparity between the need to analyze tens of thousands of alerts daily and allocating only one


---


3 The National Cyber Directorate, Implementation Guide for the Organization's Cyber Defense Version 2.0 (June 2021).







analyst to the SOC. This situation raises concerns regarding the timely identification of genuine threats or at all.

 **Business Continuity** – deficiencies were found in the NII's business continuity capabilities across several critical areas. The current draft business recovery procedure lacks essential elements typical of a comprehensive business continuity plan, including up-to-date mappings of vital processes and associated risks, clearly defined recovery objectives, and allocating necessary resources. Moreover, the draft procedure contains recovery priorities established in 1991 and ratified in 2013, which are outdated. Furthermore, the NII has not conducted a disaster recovery drill in the past three years, and gaps were found in restoring data from backups.

 **Supply Chain Risk Management** – the NII does not have a formal supply chain procedure or a comprehensive mapping of its ICT suppliers and their risk classifications. Additionally, the tenders it issued do not include an information security appendix that mandates supplier compliance with controls aligned with the supply chain methodology requirements. Moreover, the NII does not audit its ICT suppliers, which presents a risk to the organization due to potential vulnerabilities in critical suppliers. In the few instances where audits have been conducted, deficiencies were identified.

 **Transfer of Information from the NII to External Bodies** – the NII shares information with numerous external bodies via information-sharing systems with security gaps. Furthermore, the NII does not ensure that the information shared with public bodies aligns with the approval given by the Information Transfer Committee. There is also a lack of periodic audits regarding the expiration of information transfer interfaces, which leads to continued information sharing beyond the five-year limit specified in its procedures.

 **Compliance with Legal and Regulatory Requirements** – the NII does not have a work plan for a continuous monitoring of its databases adhering to the Protection of Privacy Regulations, as mandated by Regulation 3 to said Regulations. Given that the NII database, classified as an extensive database, contains sensitive information of many terabytes, it is mandatory to implement such an organized plan to achieve an adequate level of security. Furthermore, 87% of the Protection of Privacy Regulations (13 out of 15) are only partially complied with by the NII.



**Internal Penetration Testing Team** – the NII employs a dedicated team of trained resilience testers who routinely conduct infrastructural and applicable penetration tests for various systems and applications. Still, no tests are performed on the central system.

**Supply Chain** – in the new tenders, the NII has incorporated requirements for supplier audits and their obligation to report incidents in the information security chapter.








**The Iron Swords War** – during the Iron Swords War, the NII undertook urgent measures to assist victims of hostilities, families of the hostages, families of evacuees, and reserve personnel. These measures included developing new services for these populations, creating interfaces for information transfer to other entities, and implementing solutions enabling NII's employees to work remotely to ensure uninterrupted service.







**Backup Site (DR)** – the State Comptroller's Office commends the NII for relocating the backup site (DR) to a new location in March 2024, during the audit.

---

## Key Recommendations

-  The NII should revise its information security and cyber protection policy document to address issues that require attention according to established standards and present the updated document to the Information Security Steering Committee. Furthermore, it should periodically update the document to align with evolving risks, as mandated by the NII Security and Cyber Protection Policy.
-  Given concerns that critical issues in the NII's information security are not addressed according to changes in the organizational environment and emerging cyber threats and risks, the NII should update its information security procedures to encompass the obligations set forth by the Information Security Regulations. Additionally, existing procedures that have not been revised in the last two years require updating.
-  Following the replacement of the acting CEO at the NII after the first Cyber Steering Committee meeting, and considering that significant issues such as the level of cyber protection were not discussed during the committee's session, the NII should reconvene the Cyber Steering Committee promptly. This meeting should focus on presenting the cyber protection levels and other key issues outlined in the committee's appointment letter and obtaining approval for the draft policy.
-  The NII should catalog all its assets and business processes, classify them according to their importance to the organization and adhere to the requirements of the Information Security Regulations.
-  With guidance from the National Cyber Directorate, it is recommended that the NII systematically conduct information security risk surveys following accepted methodologies, such as the protection doctrine, and ensure that the risk surveys consider risks posed to Critical Cyber Infrastructure bodies on the national level. The results and a plan to address identified deficiencies should be submitted to the National Cyber Directorate, which functions as the professional supervisor of the NII.



-  The NII should engage content experts to conduct penetration tests on the central system. Given that some CCI bodies have comparable systems, the National Cyber Directorate should establish a forum to facilitate knowledge sharing among relevant parties, which will also evaluate a national systemic response for testing these systems.
-  The establishment of dedicated crisis management teams, including an incident response team (IR) and a digital forensic and incident response team (DFIR), is recommended for the NII. Additionally, the NII should convene and train the management team to handle cyber incidents effectively.
-  In collaboration with the National Cyber Directorate, the NII should enhance the capabilities of its Security Operations Center (SOC) to detect and respond to cyber incidents while also addressing operational gaps within the SOC. It is further recommended that the SOC be subordinate to the Information Security Division.
-  With assistance and guidance from the National Cyber Directorate, the NII should perform a comprehensive mapping of its suppliers under the recommendations of the National Cyber Directorate. It is also recommended that a template for an information security appendix be developed for tenders, outlining the supplier's contractual obligations and compliance requirements under the National Cyber Directorate's supply chain methodology.
-  Risk assessments and information security audits should be conducted for active information-sharing systems. When information security vulnerabilities are identified, the NII should implement compensating controls.
-  The NII should expedite an audit of compliance levels of significant databases it holds concerning the Information Security Regulations in line with regulatory requirements. This audit should be conducted regularly.



## The National Insurance Institute's Level of Compliance with the Information Security Regulations

Topic	The audit findings
Database definitions document	Partially found
Information Security Officer	Partially found
Security Procedure	Partially found
Mapping of the database systems and performance of a risk survey	Partially found
Physical and surroundings security	Found
Information security with respect to management of manpower	Partially found
Logical protection – topic 1	Partially found
Logical protection – topic 2	Partially found
Logical protection – topic 3	Partially found
Documenting of security incidents	Partially found
Mobile devices	Partially found
Secured and updated management of database systems	Partially found
Communications security	Partially found
Outsourcing	Partially found
Periodic audits	Not found

Prepared by the Office of the State Comptroller.



---

## Summary

The NII maintains an extensive database containing many terabytes (TB) of information regarding all residents of the State of Israel from birth to death. It is imperative to ensure a high level of security for this database, in compliance with the Privacy Protection Law and the Privacy Protection Regulations, due to its classification as a primary target for potential attacks, with tens of thousands of suspected incidents occurring daily. The potential damage to this database is critical, especially during the ongoing conflict known as the Iron Swords War, during which the NII has a crucial role in supporting the injured, evacuees, and reservists.

In June 2023, the NII was designated as a Critical Cyber Infrastructure body (CCI body) and commenced processes to enhance its cyber defense under a dedicated doctrine for CCI bodies and the guidance of the National Cyber Directorate. During the Iron Swords War, the NII implemented urgent measures to assist victims of hostilities, the families of the hostages, evacuees, and reservists. These measures included developing new services for these populations, creating interfaces for information transfer to other entities, and identifying solutions that allow staff to work remotely, thus ensuring uninterrupted service delivery.

This report's findings highlight significant deficiencies in information security management at the NII and its preparedness for cyber threats. Numerous gaps were found across all areas pertinent to information security, including deficiencies in the detection and management of cyber incidents, inadequate logical security measures, an outdated business continuity plan, and low recovery capacity in the event of a disaster. Collectively and individually, these findings risk the information's confidentiality, integrity, and availability within the NII databases.

Additional findings indicate only partial compliance with the Information Security Regulations and a lack of capacity within the organization's information security division to fulfill specific responsibilities.

The Acting CEO of the NII, the management team, the Cyber Steering Committee, and the National Cyber Directorate, as the professional guide, should identify the material cyber risks facing the organization and develop a comprehensive work plan to address the information security gaps highlighted in this report.





Report of the State Comptroller of Israel – Cyber and  
Information Systems | November 2024

The National Insurance Institute

---

# **The Tevel Project for Upgrading the Computing Systems in the National Insurance Institute – Follow-up Audit**







# The Tevel Project for Upgrading the Computing Systems in the National Insurance Institute – Follow-up Audit

## Background

In 2009, the National Insurance Institute (NII) initiated the "Tevel" Project to upgrade the computer system (Tevel or the Project), whose main goal is the realization of the principle of "the insured at the center," which focuses on the exhaustion of his rights. The Project is indented to progressively enhance the core and main headquarters systems of the NII, encompassing 48<sup>1</sup> systems and subsystems, and establish a modern technological infrastructure. The planned duration of the Project was 11 years, from early 2010 to the end of 2020, and its total budget was planned to be about NIS 477 million.

In 2015, the State Comptroller published a report addressing phase A<sup>2</sup> of the Project (the State Comptroller's Report from 2015), which noted, inter alia, that given the deviations from the project's budget and schedule, it is necessary to rectify the deficiencies to ensure that in the coming years, the implementation will continue in alignment with approved plans and content in subsequent years. The report underscored the importance of completing the Project without further delays, given that one of its primary objectives is to place the insured's needs at the center and the exhaustion of his rights. In 2017, a report from NII's consultants decided that the chosen implementation approach was flawed, compounded by an overall failure in program management. Their principal recommendation was to continue executing the Project plan while limiting it to partial content relative to the original plan.

In 2020, the State Comptroller's Office published another report on the "Tevel" Project<sup>3</sup> (the Previous Report or the Previous Audit), criticizing the management of the Project's content, budget, and work plan, including the necessary rectification of deficiencies highlighted in the State Comptroller's Report from 2015. The said Report concluded that although the NII had implemented several essential and advanced systems contributing to enhanced work processes and improved service for the insured, these systems constituted only a tiny fraction

1 In the previous audit 31 core systems were noted. Given their size and scope of modules of the Medical Committees System (Such as the system of work injury or general disability committees) they are regarded in the follow-up audit as separate systems, therefore there are 38 core systems. Moreover, the project included ERP system with ten modules in the headquarters. Thus, in total 48 systems and subsystems.

2 See the State Comptroller, Annual Report 65C (2015), "The Tevel Project for Upgrading the Computing Systems in the National Insurance Institute", pp. 1289–1331.

3 See the State Comptroller, Annual Report 70C (2020), "The Tevel Project for Upgrading the Computing Systems in the National Insurance Institute".



of those planned in 2009. The pathway to fully realizing the project's main objective – the implementation of the "insured at the center" concept – remained distant. The primary recommendation was for the National Insurance Institute to reassess the evaluation and planning procedures within the Project thoroughly and to closely monitor progress toward meeting milestones at each stage to mitigate further delays in its implementation.

In 2021, a decision was made to reduce the Project scope further, focusing specifically on the domain of pensions – specifically, types of pensions requiring the convening of medical committees for their approval, while suspending the addressing of other core systems. Later that year, the NII sought the expertise of an additional consultant to evaluate the Project's continuation. The consultant identified significant delays in schedules and substantial cost overruns compared to initial plans; However, he also noted improvements in the Project's management. The consultant recommended continuing the Project, emphasizing the necessity of strengthening budgetary control processes.



### Key Figures

**14 years**

since the beginning of the project in 2010, planned to be completed in 2020. By the end of the current multi-year plan (in 2025), the Project will be five years behind schedule with no expected completion date

**NIS 1 billion**

the expected cost overrun of the Project by the end of the current multi-year plan. This overrun is expected to increase by hundreds of millions of NIS by the time the Project is completed

**200%**

the expected increase in the Project cost compared to its original budget until the end of the current multi-year plan. From a planned NIS 477 million to an expected NIS 1.5 billion

**50%**

of the core systems (19 out of 38) were removed from the Project, and their implementation was suspended, such as the systems that handle old-age and survivors' pensions, reservists, and children

**51 years**

the age of the information system that handles old-age and survivors' pensions. This system and other systems developed decades ago were removed from the Project

**270,000**

insured individuals were treated through the "Tevel" system in 2022, 140,000 claims were filed, and 50,000 medical committees were held through the system

**only 10 systems**

of the 38 core systems originally planned to be completed in 2020 were implemented by the follow-up audit time (26%)

**NIS 116 million**

the average annual budget of the "Tevel" Project in 2019–2023

### Audit Actions

From June to September 2023, the State Comptroller's Office followed up on the key deficiencies of the Previous Audit concerning the "Tevel" Project. This follow-up audit was carried out at the National Insurance Institute (NII), and focused on the project budget, implementation timelines, and contents. Additionally, the audit included an assessment of the multi-year and annual work plans, their supervision, and the Project's budgetary control.



## Key Findings



**The Delineation of the Project and the Contents that were Implemented** – the Previous Audit noted that the NII had only executed a small portion of the systems initially planned for inclusion in the Project in 2009. **The follow-up audit found that the deficiency was slightly rectified.** NII has decided to detract 19 (50%) of the 38 core systems from the Project, with 6 systems removed since the Previous Audit. Nine additional systems (about 24%) remain unrealized. Seven systems have been fully implemented, comprising 3 new systems and 4 that were partially operational during the Previous Audit. Only 10 of the core systems (about 26%) were fully implemented under the Project. Moreover, six out of ten modules within the ERP project have not been implemented, and the NII does not plan to complete the additional systems outlined in the Project beyond 2025.



**The Project Timelines** – as of the audit end date, fourteen years since the beginning of its execution, despite a significant reduction in Project content to about half of the original plan, the substantial delay in timelines and persistent decrease in content reflect a consistent, multi-year process of distancing from the original planning of the Project to the point of relinquishing entire layers of it. This trend, which has been ongoing for several years, has not resulted in adherence to deadlines for implementation even after content reduction. As of the follow-up audit date, the completion of the multi-year plan approved for implementation until 2025 (which includes 15 of the 38 [40%] core systems initially planned) will be five years (about 45%) behind the original schedule. Moreover, the NII lacks a strategy to complete the approved limited content, leading to expectations of further schedule deviations.







The NII decided to exclude from the "Tevel" Project and not upgrade nearly 50% of the planned core systems without an alternative technological response for these systems. The systems detracted from the Project encompass areas such as old-age and survivors', reserve, unemployment, children's, and survivors' benefits, facilitating the disbursement of tens of billions of NIS to over one million insured individuals annually. These systems developed decades ago (the old-age and survivors' system was developed in the 1970s) on outdated infrastructures and technologies, face diminishing technological capabilities, and the availability of professionals to continue to maintain them is decreasing. This decision effectively alters the Project's original objective to modernize the NII's information system, eliminate technological and process barriers, enhance management and control, and improve agility in adapting information systems and processes to legislation, regulation, and NII policy changes.



**The Project Budgeting** – the Previous Audit raised that, despite partial implementation of the Project contents compared to the original plan, the budget execution rate by July



2019 was about 58% over the original budget allocation. **The follow-up audit found that this deficiency was not rectified as of the audit date;** even with significant content reduction (by about half), expenditures reached about NIS 1.2 billion, roughly 260% of the initially approved budget of NIS 477 million. It is estimated that by completing the current multi-year plan in 2025, the Project costs may exceed 200% of the original budget, resulting in an excess of over one billion NIS. Notably, the NII lacks an estimate for the anticipated costs associated with the subsequent multi-year plan, thereby failing to estimate the total Project cost upon completion.

-  **Inclusion of the Cost of NII's Standard Workforce Employees in the Project Budget** – the Previous Audit raised that the Project budget data does not include the employment costs of the NII's standard workforce employees incorporated in the Project, and it recommended that such expenses be incorporated. **The follow-up audit found that this deficiency was not rectified.** Despite the NII's management stating it would implement the recommendation, the personnel costs for these standard workforce employees were not included in the Project budget. These costs are about NIS 5 million annually, representing about 4% of the annual Project budget.
-  **Project Planning vs. Execution and Budget Control** – the Previous Audit raised that the NII's budget supervision team faced difficulties to comprehensively control over the Project budget compared to the planned one, mainly due to insufficient detailed, complete, and current planning data. **The follow-up audit found that the deficiency in the budgetary control procedures was slightly rectified.** During this audit, it was noted that in the task status control process, the NII retroactively updates the planned hours for the execution of each completed task so that these align with the actual execution hours. This practice of retroactive updating effectively nullifies the hours budget allocated for the planned execution hours within the Project, which involves the management of hundreds of tasks. Consequently, upon completing the update of performance data for the task, the planning data regarding resource allocation (number of development hours) is presented as equal to the actual performance data.
-  Disregarding planning data highlights a significant deficiency that significantly affects the overall Project supervision and control. The lack of continual monitoring of discrepancies between planning and actual execution hampers the effective management of resource allocation in the Project, which involves hundreds of thousands of development hours with a financial cost of tens of millions of NIS per year. Furthermore, the quarterly budget control report submitted to the accountant relies on planning data from the Project management system, which is retrospectively updated according to actual execution. Consequently, this report does not accurately reflect the original planning and cannot be relied upon for control or decision-making. Effective budgetary and process control is unattainable without dependable reporting on planning data, leading to potential inaccuracies in decision-making based on these reports.
-  **Conducting Research at the End of Each Version** – after each version or development cycle is completed, comprehensive investigations and lessons-learned







processes are not undertaken routinely. The NII is satisfied with performing spot investigations into specific events; However, this approach fails to address the necessity for a thorough lesson-learned process that examines the entire version lifecycle. This examination should encompass the requirements gathering stage, characterization and development processes, change management, testing, and the go-live stage. Lessons are essential for change, improvement, and preservation purposes, even when a version is successfully launched, to replicate future successes. The absence of these processes undermines the NII's capacity to enhance development processes systematically and continuously.



**The Governance Mechanisms in the Project** – the State Comptroller's Office commends the NII for the ongoing efforts of the Steering Committee and the Finance Committee, as well as the periodic meetings conducted by the accountant and ICT VP, noting that the plan has received unanimous approval from all parties involved in its execution.

---

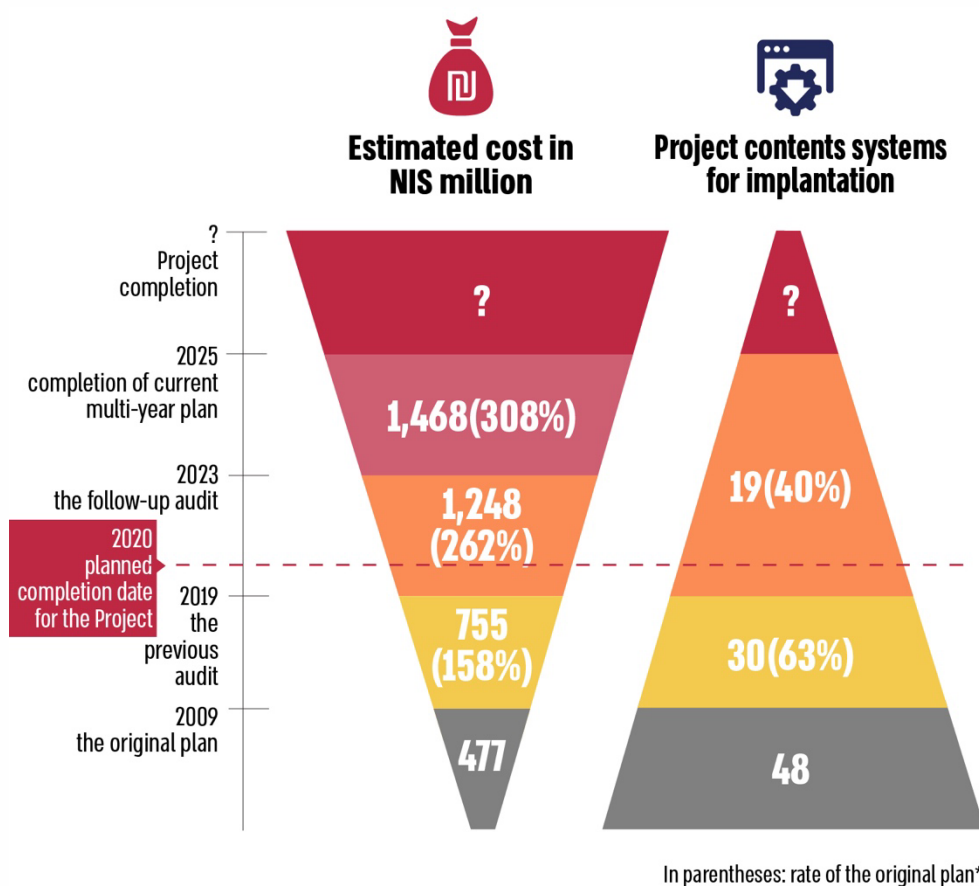
## Key Recommendations

-  The NII should develop a comprehensive plan, including a finalized schedule for the Project completion, with all components duly approved. Additionally, periodic control mechanisms must be established to ensure the effective implementation of the plan. All of this is to achieve the main goal of the Project – placing the insured and fulfilling their rights at the center.
-  The NII should assess the future of the systems excluded from the Project, considering the quality of current solutions and their technological viability for sustained operation within the existing technological framework. Based on this assessment, a multi-year upgrade plan must be formulated to achieve the principal aim of the "insured at the center" while concurrently advancing the existing systems within the "Tevel" Project.
-  Due to significant and ongoing budgetary deviations, the NII should conduct a thorough investigation to identify and analyze the causes of these deviations. It must also prevent future deviations in this and another IT Projects it manages. Following this investigation, a final budget for the Project completion must be established, along with the designation of accountability for budget adherence.
-  The NII should include in the Project budget all associated expenses, including the costs related to the employment of standard workforce employees.



- 💡 The NII should implement Standard control processes, wherein original planning is compared against actual execution. This includes an analysis of both overestimations and underestimations to facilitate the extraction of reliable lessons regarding actual costs and the efficiency of the characterization, development, and testing teams' efforts.
- 💡 The Project's management should adopt a structured and systematic approach for lessons learning after each Project version.

### The Reduction in the Contents of the "Tevel" Project Compared to the Rising Costs





---

---

## Summary

The "Tevel" Project, NII's leading digital initiative, was initiated over a decade ago to eliminate technological and procedural barriers and implement the vision of the NII to provide comprehensive access to its services for the public and promote data transparency. This initiative aligns with its principle of placing the insured at the center and maximizing their entitlements. As of the audit date, the NII has invested about NIS 1.2 billion into the Project, completing ten (a quarter) of the planned 38 core systems.

The State Comptroller's Office has published two audit reports regarding the Project's implementation: one in 2015 and another in 2020. This follow-up report examines the rectification of the key deficiencies noted in the Previous Audit.

The follow-up audit raised that most of the key deficiencies noted in the Previous Report remain unaddressed or have been slightly rectified. Schedule deviations persist, and the NII has no estimated completion date for the Project. Concurrently, while the NII reduced the Project contents by half, the current estimated cost is about NIS 1.5 billion, representing a deviation of about NIS 1 billion from the original budget of NIS 477 million (an increase of about 200%). This deviation is expected to rise by several hundred million NIS more by the Project's completion. Continuous discrepancies in Project timelines and costs adversely affect the provision of optimal services to the insured populace. The report also notes a practice of retroactively amending planning data, which significantly undermines effective supervision and budget control and examines allocated versus planned initially resources. Regarding the engagement of relevant stakeholders, the NII has addressed the deficiencies noted in the Previous Report by initiating steering committee meetings and periodic control meetings involving its management representatives.

Despite the investment of over NIS 1 billion of public funds into the "Tevel" Project – over double the initial overall planning – the objective of enhancing public services and assisting individuals in exhausting their rights has been partially realized, partly due to the Project's reduced contents.

The significant deviations in the Project necessitate the NII's administration to monitor the factors contributing to these discrepancies, establish mechanisms to mitigate them, and definitively determine the Project's completion date and budget. The management of the NII is responsible for effectively utilizing public funds invested in the Project. It is therefore recommended that the NII implement the insights gained from addressing the deficiencies outlined in this report across all Projects under its supervision. Moreover, the management should assess, given the progress of system development over the past 14 years, the expectation of achieving an improvement in the ICT response in all the systems across all of the NII's systems, particularly those excluded from the Project, and convene a thorough and strategic discussion based on examination results.






### The Rectification Extent of the Key Deficiencies Noted in the Previous Report

The Audit Chapter	The Audited Body	The Deficiency in the Previous Audit Report	The Rectification Extent of the Key Deficiency Noted in the Follow-up Audit			
			Not Rectified	Slightly Rectified	Significantly Rectified	Fully Rectified
Managing the Project's annual work plan	NII	In the first half of 2019, the NII advanced the implantation of the Project without reaching an agreement among the parties involved regarding the existence of a detailed annual work plan.				
The Project scope	NII	Only five of the 38 core systems included in the original 2009 Project contents had been implemented by August 2019, and even then, only partially compared to the original plan. Of the 10 modules in the headquarters (ERP system), only two were fully implemented, and one was partially implemented.				



The Audit Chapter	The Audited Body	The Deficiency in the Previous Audit Report	The Rectification Extent of the Key Deficiency Noted in the Follow-up Audit			
			Not Rectified	Slightly Rectified	Significantly Rectified	Fully Rectified
The Project budget	NII	Although the NII established a budget supervision team in 2018 which met regularly, the team had difficulty thoroughly monitoring the Project budget in 2019 compared to the planned contents due to the lack of detailed, complete, and updated planning data.				
The Project budget	NII	Despite partially implementing the Project's contents compared to the original plan, budget execution by July 2019 was about 58% over the original budget approved for the Project in 2009 (about NIS 755 million compared to the original budget of NIS 477 million).				



The Audit Chapter	The Audited Body	The Deficiency in the Previous Audit Report	The Rectification Extent of the Key Deficiency Noted in the Follow-up Audit			
			Not Rectified	Slightly Rectified	Significantly Rectified	Fully Rectified
The Project budget	National Insurance Institute	The Project budget execution data does not include all direct costs, such as salaries for 15 ICT and information systems administration employees employed on the Project.				





Report of the State Comptroller of Israel – Cyber and  
Information Systems | November 2024

Government Defense Industries

---

# **Cyber Security: Aspects of Regulation and Protection of the Information and Computer Systems at Rafael Advanced Defense Systems Ltd.**





## Cyber Security: Aspects of Regulation and Protection of the Information and Computer Systems at Rafael Advanced Defense Systems Ltd.

### Background

According to the government's resolution in August 2011<sup>1</sup>, the Israeli civil cyberspace encompasses all state and private entities within the State of Israel, excluding special entities<sup>2</sup>. Consequently, the Israeli cyberspace integrates civil, governmental, and Military Cyberspace domains. The increasing activity within the Cyberspace domains facilitates technological innovation and advancements beneficial to individuals and their environments. However, a significant challenge has emerged alongside the advantages of computerized systems in cyberspace: the cyber threat. A cyber incident is defined as an occurrence suggesting potential harm to the regular operation of a computer system. Rafael Advanced Defense Systems Ltd. (Rafael) enhances the nation's military strength and resilience. The company is subordinated, among others, to the provisions of the Government Companies Law, 1975, and the Regulation of Security in Public Bodies Law, 1998. The Director of Security of the Defense System (MALMAB) supervises enterprises within the defense system<sup>3</sup> and those manufacturing products for this sector. The Government Companies Authority disseminates circulars to government companies and subsidiaries on various matters under its authority under the Government Companies Law, 1975, encompassing corporate risk management.

In 2022, the National Cyber Directorate (NCD) received reports of 9,108 cyber incidents from all entities nationwide, with about 31% of these incidents attributed to phishing attacks<sup>4</sup>.

1 Government Resolution 3611 (August 7th, 2011).

2 Government Resolution 3611 (August 7th, 2011) defined special entities as follows: the IDF, the Israel Police, the Israel Security Agency (ISA), the Mossad Institute for Intelligence and Special Operations (Mossad), and the defense establishment through the Director of Security of the Defense Establishment (MALMAB). Additionally, the defense establishment was defined as follows: the bodies directed by MALMAB by virtue of the Regulation of Security in Public Bodies Law, 1998, as well as suppliers and enterprises developing or manufacturing defense equipment for them.

3 The Defense Establishment – the IDF and the Ministry of Defense (MOD), including its auxiliary units.

4 Phishing – A cyber-attack in which the attacker poses as a trustworthy entity in order to deceive people and make them reveal sensitive information.



## Key Figures

**10%**

in 2022: the budget for the Technology Security and Cyber Defense Department at Rafael out of the computing budget of the Information Technology and Processes administration at Rafael

**12 years**

the NCD and the Director of Security of the Defense System did not implement the government's resolution on promoting national capability in cyberspace regarding the establishment of special arrangements for promoting cyberspace defense

**31%**

the phishing cyber rate incidents reported to the NCD in 2022 out of all cyber incidents

## Audit Actions



From November 2022 to July 2023, the State Comptroller's Office audited the cyber Security regulating and protecting information systems at Rafael. The audit focused on the following issues: the regulation of the working relations between the National Cyber Directorate and the Director of Security of the Defense System; The directive and supervisory powers of the Director of Security of the Defense System; The concept of cyber defense at the Director of Security of the Defense System; Rafael's information security policy; Corporate risk management at Rafael; Rafael's cyber defense work plans and budget; The protection of specific computer networks and information systems at Rafael and the information security controls implemented therein; And the safeguarding of specific infrastructures at Rafael. The audit was conducted at the Director of Security of the Defense System and Rafael. Completion examinations were performed at Israel Aerospace Industries Ltd. (IAI), Israel Electric Company Ltd., and the National Cyber Directorate (NCD).

The Knesset State Audit Committee sub-committee decided not to submit data from this chapter before the Knesset to protect the state's security and its international trade relations under Section 17 of the State Comptroller's Law, 1958 [Consolidated Version].





## Key Findings



**Regulating the Working Relations Between the National Cyber Directorate and the Director of Security of the Defense System** – even though 12 years have passed since the government's resolution in August 2011 enhancing national capacity in cyberspace, the NCD and the Director of Security of the Defense System have not implemented specific arrangements regarding the protection of cyberspace and the promotion of research and development, as mandated by the government resolution.



**The Director of Security of the Defense System's Directive and Supervisory Powers** – the Regulation of Security in Public Bodies Law from 1998 did not confer apparent authority to the Director of Security of the Defense System (MALMAB) concerning operational, technological activities, nor did it empower MALMAB to offer professional guidance on specific networks.



**The Concept of Cyber Defense Within the MALMAB** – the cyber defense doctrine as outlined by the Theory and System Defense Division in the MALMAB's technology does not incorporate a standard for an organization's monitoring center, even though such a center is a critical component of organizational defense. Furthermore, the Theory and Defense Division has not issued directives for the guided entities concerning preparedness required for managing cyber incidents or for incident management itself, which should encompass monitoring processes, incident identification, response strategies, recovery efforts, investigations, lessons learned, cyber incident simulations, internal participation in managing a cyber incident and the interfaces between them, and necessary activities of the guided entity vis-à-vis external factors.



**Corporate Risk Management at Rafael** – in May 2023, during the audit, the corporate risk management committee approved a risk strategy document and risk management policy, about three and a half years after the Government Companies Authority's circular on corporate risk management was published in January 2020. However, these documents were not approved by Rafael's board of directors. As of July 2023, the risk management policy lacked provisions for reporting mechanisms to external parties. Additionally, Rafael has not reported as required to the Government Companies Authority, contravening the circular's corporate risk management stipulations.



**Physical Protection for Certain Infrastructures** – gaps have emerged in this field.








**Cyber Incidents Insurance** – as of July 2023, during the audit, Israel Electric Company Ltd. held two insurance policies for property damage and third-party claims related to cyber incidents. Israel Aerospace Industries Ltd. (IAI) and Rafael<sup>5</sup> lacked such

5 Except for Rafael's IT equipment and computer systems that are insured against a cyber incident originating from an error or omission.







policies. Rafael did not purchase insurance against cyber incidents mainly for the following reasons: Rafael's level of cyber protection is high, purchasing insurance is economically inefficient, it is unlikely that compensation will be granted by the insurance company for damage to production or sales turnover, classified information cannot be disclosed to the insurance company following damage due to a cyber incident, complicating the claims process, and insurance coverage is limited to a maximum of ten million dollars, an amount that is not material to Rafael's operations.

-  **Reporting Gaps at Rafael** – Rafael failed to disclose several cyber incidents to its board of directors during meetings as required.
-  **Investigating Cyber Incidents** – Rafael's management failed to investigate cyber incidents that occurred between 2020 and 2022 concerning certain aspects critical to Rafael's operational integrity.
-  **Comprehensive Plan for the Management of Information Security Incidents** – the Detailed, Information, and Process Administration Order from February 2023 does not delineate the recovery process for specific cyber incidents, nor does it reference a defined plan or include pertinent documentation.
-  **Deriving Lessons from Certain Cyber Incidents** – several incident investigation documents did not sufficiently address the lessons derived therefrom.
-  **Surveys and Penetration Tests** – Rafael has not set the frequency for conducting mandated surveys and penetration tests, resulting in inconsistencies in this area.

---

## Key Recommendations

-  The NCD and the Director of Security of the Defense System should adhere to the government's resolutions concerning the regulation of their cooperation through the established mechanisms.
-  The MALMAB should regulate the powers required to fulfill its mission effectively.
-  It is recommended that the technological unit of the MALMAB finalize the cyber defense doctrine, including the standards for the monitoring center and the necessary guidelines for managing cyber incidents and occurrences, conducting investigations, and deriving lessons learned.
-  Rafael's management should provide the board of directors with required updates related to cyber incidents.



- 💡 Rafael's management Should annually assess the budget needed for cyber defense concerning potential damage, annual sales turnover, and annual operating profit.
- 💡 Rafael's management should investigate cyber incident management as mandated. Rafael should complete the guidelines for technology security incident management and cyber protection in computer systems.
- 💡 Rafael is recommended to address the deficiencies identified in surveys and penetration tests.
- 💡 Rafael should rectify the deficiencies highlighted in this report.

---

## Summary

Rafael is a significant component in enhancing the country's military strength and resilience. The audit raised deficiencies related to, among other issues, the lack of regulation in the working relations between the National Cyber Directorate (NCD) and the Director of Security of the Defense System (MALMAB) and safeguarding information and computer systems at Rafael. Rafael's management and board of directors should address these deficiencies and ensure, in collaboration with the MALMAB, that Rafael adheres to the directives of the MALMAB as required.





Report of the State Comptroller of Israel – Cyber and  
Information Systems | November 2024

Special Report

---

# **Artificial Intelligence – National Preparedness**





# Artificial Intelligence – National Preparedness

## Background

Artificial intelligence (AI) is an overarching term for technologies developed to enable machines to execute tasks that necessitate human intelligence. The ongoing AI revolution is recognized as a "disruptive innovation" poised to alter various aspects of life and numerous industries significantly. The Ministry of Innovation<sup>1</sup>, Science and Technology (the Ministry of Innovation) defines AI as "the capability of a machine to learn to perform human actions and enhance its performance, relying on data, examples, and operational experience, and, in a broader context, all technological operations extracting information and insights from databases."

Academic research in artificial intelligence dates back to the 1950s. However, in recent years, particularly following the introduction of various tools and applications (apps) available in the market for diverse fields, there has been a marked advancement in the integration capabilities between man and machines, which some characterize as a genuine revolution. AI is employed in various sectors, including the development of autonomous vehicles, analysis of X-ray images, assessment of credit risks, securities trading, and candidate evaluation for employment. Furthermore, AI systems play integral roles in interactions between consumers and businesses, businesses and other businesses, professionals and clients, labor relations, public sector entities, and the public and general public.

AI was also widely used during the "Iron Swords" War; apart from its operational use, it contributed to the identification and location of hostages and fatalities. In advocacy, AI facilitates the creation of multilingual videos, enhancing accessibility to diverse populations worldwide through voice reproduction, animation, dubbing, subtitles, and translation. Additionally, the war highlighted the use of "deepfake" technology – a form of AI utilized by various parties for propaganda and the dissemination of misinformation.

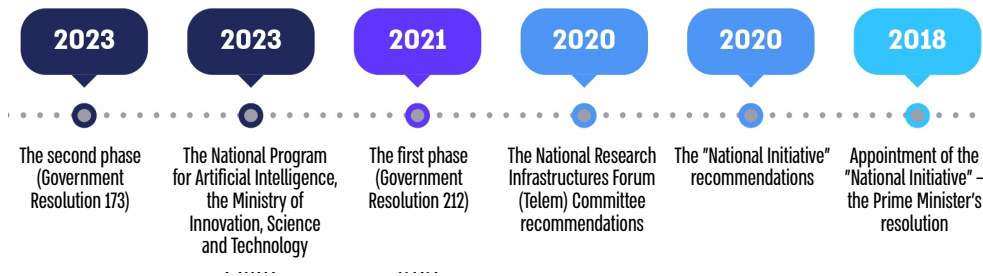
In May 2018, the Chief of Staff for the National Security Council at the time, following the Prime Minister's directive, appointed project leaders to formulate a national plan to bolster scientific-technological resilience as a critical component of Israel's national security ("the National Initiative"). Thus positioning Israel globally among the top five countries in core technological domains, including artificial intelligence and data science. The Initiative's report was presented to the Prime Minister and published in September 2020.

---

<sup>1</sup> Breakthrough innovation that brings about a fundamental change and often threatens the existing one.



## Artificial Intelligence in Israel – Milestones in 2018–2023



In February 2020, the Chairman of the National Research Infrastructures Forum (Telem Forum<sup>2</sup>) appointed a professional review committee led by Dr. Orna Berry to assess the necessity for government intervention to accelerate advancements in artificial intelligence and data science (Telem Committee). The Committee's directive, outlined in the appointment letter, emphasized the importance of focusing on the following aspects: human capital, physical infrastructure, access to databases, and knowledge transfer from academia to industry. The Committee's findings were published in December 2020. In August 2021, following Government Resolution 212, the government approved the Telem Committee's recommendations, initiating the first implementation phase with a budget of about NIS 550 million from 2021 to 2023.

In July 2022, the then-Minister of Innovation launched a "National Program for Artificial Intelligence". This program, crafted by an inter-ministerial team, was officially published by her ministry in January 2023 (the Ministry of Innovation's National Program).

In February 2023, Government Resolution 173 approved an extension to the first phase, approved in August 2021 (the second phase). This resolution included a directive to the Ministry of Finance to allocate a budget not exceeding NIS 500 million, which will be utilized by Telem Forum entities from 2023 to 2026.

This audit report evaluates the national preparedness in artificial intelligence, examines how the Israeli government formulates and enacts a national strategy to position Israel among the leading countries globally, and assesses whether its actions in artificial intelligence will establish a robust foundation for Israel's development and prominence as a scientific and technological power. The preparedness, decision-making, and implementation processes for the government program in artificial intelligence commenced in 2018 and continued throughout the audit period.

2 A voluntary action framework designed to coordinate and pool resources among all national bodies that may benefit from a large research infrastructure (the Directorate of Defense, Research, & Development (DDR&D), the Planning and Budgeting Committee, the Ministry of Finance, the Innovation Authority, and the Ministry of Innovation).





## Key Figures

### 0

Israel has no **long-term national strategy** in artificial intelligence. The government did not approve a **comprehensive and individual master plan for the implementation**. Instead, over the years, it has approved programs in phases implemented slow, lacking, and does not meet the set schedules

### only 1 NIS billion

was approved by the government in two phases. most of the amount had not yet been realized. The approved budget is about a fifth of the recommended one by the Telem Committee in December 2020 and about a tenth of the "National Initiative" recommendation from September 2020

### drop from 5th place to 9th place

in the Tortoise index out of 83 countries in 2019–2024. This is an international artificial intelligence, index whose ranking is based on – investment, innovation, and application

### drop from 20th place to 30th place

in the Oxford index out of 193 countries in 2020–2023. This is an international artificial intelligence index regarding governmental readiness for artificial intelligence. In a sub-index measuring the government's artificial intelligence strategy and its digital capabilities, Israel dropped 33 places (from 35th to 68th) in these years

### only 40%

was realized of the first phase budget, the government approved for 2021–2023 (NIS 220 million out of about NIS 550 million). The realization rate refers to agreements that have been signed, of which tens of millions of NIS have not yet been executed or completed

### only 11%

the realization rate of the first phase in high-performance computing (supercomputer), which is about NIS 30 million out of the NIS 270 million approved

### 55%

of the budget allocated in the first phase for human capital was realized (about NIS 34 million out of NIS 62 million), focusing on the needs of academia but not to the industry needs

### 76%

the budget realization rate in natural language processing in Hebrew and Arabic. However, the realization rate includes an agreement for a language module for which there is a budgetary commitment that has not yet been realized



---

## Audit Actions



From June 2023 to March 2024, the State Comptroller's Office examined the national preparedness in artificial intelligence, assessing Israel's international ranking and the government and relevant ministries' actions to advance a national program for artificial intelligence. The audit was performed in the Ministry of Innovation, the Innovation Authority, the Ministry of Defense, the Planning and Budgeting Committee, the Ministry of Finance, and the National Security Council in the Prime Minister's Office. Supplementary examinations were conducted within the National Digital Agency at the Ministry of Economy and Industry.

---

## Key Findings



**The Absence of an Integrating Government Body Supervising Artificial Intelligence National Program** – under the government's resolution and the agreement reached between the Minister of Innovation and the head of the National Security Council in July 2022, the Ministry of Innovation, under the then minister's leadership, formulated a national program for artificial intelligence. However, after the change in government in January 2023, the Ministry of Innovation did not comply with the government's resolution to promote and lead in artificial intelligence. The program initiated by the Ministry did not progress to the implementation phase after establishing the 37th Knesset, leading to stagnation on the established milestones. Since the change in government, the Ministry has limited its focus to specific issues within Israel's artificial intelligence sector and has not led to advancement at the national level.



Six years after the Prime Minister decided to promote artificial intelligence and submit it as a program for government approval, an overall national program to advance it has yet to receive government endorsement. Aside from the two phases of the Telem program, the national program introduced by the then-Minister of Innovation in July 2022 remains ineffective when it has not been implemented following the change in government. The necessity for the government's approach to artificial intelligence to be guided by an integrating government body responsible for the execution of the government program is underscored by several factors: the significance of this sector to the national economy and its resilience; The myriad of government ministries and public agencies engaged in the advancement and integration of artificial intelligence technology within the governmental framework; The critical importance of Israel's standing as a global leader in this technological revolution; And the mandate assigned to the Ministry



of Innovation to supervise the government's strategy. As of the audit date, there is no integrating government entity that holds overall responsibility for formulating and leading a national program, pooling budgets, and controlling and supervising the program's implementation and progress.

**The Drop-in Israel's Ranking in Artificial Intelligence** – Israel aspires to be a leading technological and high-tech player. The audit raised that in 2019–2024, Israel's position in global rankings for activity and investment in artificial intelligence declined. The Tortoise Index dropped from 5th place out of 62 countries to 9th place out of 83 countries. The Oxford Index's ranking dropped from 20th to 30th place out of 193 countries. Additionally, in the Innovation Index, Israel's ranking dropped from 10th place to 15th place out of 133 countries. This decline is attributed, in part, to the findings detailed in this report regarding the government's approval, leadership, and execution of a broad national program in artificial intelligence. Tortoise sub-index data for 2024 indicate that while Israel excels in human capital, research, and development, it lags in government strategy (32nd place), infrastructure (26th place), and operational environment (65th place). The decline in Israel's international rankings in 2019–2024 highlights the urgent need for the government to reassess its policy regarding artificial intelligence.

**Government Discussion on the "National Initiative" Recommendations** – the "National Initiative" was established at the appointment of the National Security Council per the Prime Minister's directive. Its draft report was presented to the Prime Minister in May 2019, and the final draft was submitted to the head of the National Security Council in December of the same year. Following the changes in government that year, the final report, which included a comprehensive plan for formulating a strategic national response to artificial intelligence and associated projects with a budget of NIS 10 billion, was distributed to all government ministries and made public in September 2020. The report, compiled with input from hundreds of knowledge experts who volunteered their expertise for about two years, identified the promotion of artificial intelligence as critical for Israel's resilience across various sectors, including science, economy, security, and health. The audit found that the Initiative's recommendations were neither presented to the government nor discussed within any authorized government forum, nor were they budgeted or matured for implementation, despite the National Security Council being required to review the "National Initiative" following its completion and implementation for the review of the authorized body which approved the designation. Additionally, according to the agreement with the Legal Counsel to the Prime Minister's Office, the National Security Council was to establish the inter-ministerial team and submit its recommendations to the Prime Minister and government shortly after the "National Initiative" work was concluded, not about a year and a half later.

Once the Prime Minister, the government, or any other governmental body tasked professional parties to conduct staff work and submit a report based on the recommendations of 14 professional teams and hundreds of knowledge experts, which was to serve as a basis for making an operative decision on a specific issue, the head of



the National Security Council should have completed the process until the government discussed the recommendations following the teams' work and the submission of the report summarizing their findings; However, this did not occur. The failure to forward to the government the conclusions of the "National Initiative" report, which remained unaddressed for two years due to administrative delays unrelated to the Initiative's work, adversely impacted the government's ability to capitalize on the contributions of the exceptional knowledge experts appointed under the Prime Minister's decision.

**👇 Government Discussion of the Recommendations of the Artificial Intelligence and Data Science Committee (Telem Committee)** – the chairman of the Telem Forum appointed the Telem Committee to assess the necessity for government intervention to expedite the development of artificial intelligence and data science. It was determined that akin to the "National Initiative" recommendations intended to serve as a basis for a government decision, this program, which was completed in December 2020, was not thoroughly discussed within the government but rather in a limited manner under two phases, which were budgeted at around one-fifth of the Committee's recommended budget, at about NIS 1 billion. Consequently, it was not endorsed as a comprehensive master plan nor budgeted with a long-term vision.

**👇 Regulation** – despite the inherent risks associated with artificial intelligence technology and the imperative to regulate its usage responsibly while upholding fundamental rights, it has been determined that as of the audit end date, the collaborative efforts between the Ministry of Innovation and the Ministry of Justice to advance regulation in artificial intelligence and the principles outlined in the Policy Principles document have not yet received government approval. Israel currently lags behind the European Union, which has already enacted legislation regulating artificial intelligence use based on risk levels. The absence of regulation in Israel presents various risks that generate new legal and regulatory challenges. It is essential to ensure that, irrespective of technological advancements, human beings remain central to decision-making and that the development and application of artificial intelligence are conducted responsibly, safeguarding fundamental rights and public interests, including human dignity, privacy, equality, non-discrimination, and complete transparency.

**👇 High-Performance Computing (HPC)** – although the necessity for supercomputing infrastructure was identified in 2020 as fundamental for positioning Israel as a leading nation in artificial intelligence, five years later, existing computing infrastructures remain limited and inadequate for advancing research and industry in Israel. This deficiency in computing infrastructure hinders the public sector, academia, and industry's capacity to foster and develop artificial intelligence.

**👇 Infrastructure for Training Large Models** – it was found that by the end of December 2023, as the first phase concluded, the Directorate of Defense, Research, & Development (DDR&D) did not fulfill its obligations within the partners' agreement to establish an infrastructure for training large models. The Innovation Authority has not



yet regulated a complex calculation infrastructure for scientific use, essential for furthering artificial intelligence technology. Thus, the implementation rate of the first phase for advancing artificial intelligence stood at merely 11%, with about NIS 30 million disbursed out of a total approved budget of NIS 270 million.

**👎 Natural Language Processing (NLP)** – the Telem Committee highlighted the importance of advancing natural language processing, deeming it essential for employing artificial intelligence capabilities in government ministries and various industries. Therefore, the Program's primary objective is to bridge the significant technological divide between existing capabilities in English and other Latin languages and those in Hebrew and Arabic, the following findings were found:


- Only on December 31, 2023, the final day designated for the implementation of the initial phase, the DDR&D entered into an agreement of NIS 37 million for developing a Hebrew and Arabic language model project in collaboration with an international company. The first model is anticipated to be implemented by mid-2025, a year and a half after the conclusion of the initial phase. Notably, this financial commitment constitutes about a quarter of the allocated resources for language processing within the first phase. The substantial delay by the DDR&D in advancing the large language model (LLM) for Hebrew and Arabic may severely impede governmental responses to citizens, as the anticipated model is intended to catalyze the digital transformation of the Israeli economy, particularly within the public sector, through artificial intelligence tools.
- By the end of the first phase, Israel lacked a language model in Hebrew and Arabic for government use and citizen interaction. The total budget realization for developing language processing capabilities for Hebrew and Arabic, necessary to reduce the considerable technological gap compared to English and other Latin languages, reached 76% of the approved budget for this component (NIS 138 million out of NIS 180 million). This realization rate includes the language model agreement, which has only a budgetary commitment of NIS 37 million and has yet to be realized.


**👎 Human Capital** – it was found that in human capital investment for artificial intelligence advancement, implementing the Telem Committee's program within the first phase approved by the government was partial. As of the end of 2023, only NIS 34 million out of NIS 62 million was realized, about 55% of the allocated budget, mainly addressing academic needs while neglecting industry requirements.


**👎 Employment of Researchers and Senior Faculty in Academia** – it was found that, although the partner agreement for the first phase allocated about NIS 24 million for faculty admission in academia and around NIS 20 million for dedicated research grants in AI CORE fields, these elements were not executed, by the end of the first phase, by the Planning and Budgeting Committee. Moreover, the Planning and Budgeting Committee and the Innovation Authority lack up-to-date and accurate information on the




existing number of researchers. This deficiency underscores a lack of attention to the necessary training and development of human capital in artificial intelligence, which is critical for realizing the defined objectives.

 **Scope of Scholarships** – it was found that in 2021–2023, the Planning and Budgeting Committee awarded about 50 scholarships, representing 5% of the roughly 1,000 scholarships recommended by the Telem Committee, as part of the implementation of the first phase budget approved by the government. The average annual financial scope was about NIS 10 million, significantly lower than the NIS 100 million per year recommended by the Committee. Thus, the scope of scholarships awarded during the first phase was about 10% of the suggested budget. Furthermore, the Innovation Authority and the Planning and Budgeting Committee lack information regarding the impact of these scholarship distributions on the advancement of human capital in academia in artificial intelligence.

 **Budget Realization of the First Phase** – as of the conclusion of the first phase in December 2023, the budgetary realization was only about 40% of what was approved by the government, which was NIS 220 million out of a projected NIS 550 million. This reflects the implementation of only about 5% of the Telem Committee comprehensive program, which has not been deliberated in full within the government or adequately budgeted. It should be noted that this implementation rate pertains to signed agreements, yet tens of millions of NIS remain unimplemented or incomplete.

 **The Second Phase** – the audit raised that in February 2023, the government endorsed a budget for the second phase in implementing the Telem program, at NIS 500 million, to be executed from 2023 to 2026. However, only in September 2024, over a year and a half after the government's resolution, was the Telem Forum partners agreement signed for implementation from 2024 to 2027. This state of affairs, where the signed partner agreement mandates that the second phase is to commence about one year after the designated implementation date, signifies a substantial gap in adhering to the government's resolution regarding the second phase. This, among other things, given the assessment that in the first and second year out of the four that the government decided upon, only about 10% of the total budget stipulated in the government's resolution will be realized within the framework of the agreement.

It should be noted that the total budget approved for both the first and second phases was about NIS 1 billion, about one-fifth of the budget recommended by the Telem Committee in December 2020.

 **Data Literacy** – the findings indicate that, although data literacy is a crucial skill anticipated to be necessary across various fields and sectors, neither the first phase approved by the government nor the partners' agreement for the second phase addressed this area. Furthermore, the Ministry of Education was not included in the partner agreements promoting artificial intelligence. This omission of data literacy





education at an early age could hinder the readiness and integration of the next generation into the technological landscape, as artificial intelligence increasingly concerns all aspects of life and is expected to be utilized daily by the general public.









**Establishment of a Knowledge Center in the Ministry of Innovation** – the State Comptroller's Office commends the Ministry of Innovation for engaging various entities to promote regulatory principles and establishing a knowledge center focused on the regulation and ethics of artificial intelligence.

## Key Recommendations

-  The Ministry of Innovation should adhere to the government's resolutions and the conclusions reached with the then-Minister regarding collaboration with the National Security Council, thereby leading the government's policy on artificial intelligence. Within this framework, finalizing the national strategic program initiated in 2022 is essential. This program should encompass, among other elements, a vision, milestones, a comprehensive action plan detailing the government bodies responsible for each action direction, timelines for implementation, and a corresponding budget plan. Additionally, it should establish a framework for the periodic evaluation of the state's adherence to the objectives outlined in the plan, as well as mechanisms for individual evaluations of the defined action directions, including updates as necessary. The Ministry of Innovation, Science and Technology is currently tasked with fulfilling its responsibilities, thereby upholding the government's resolution. Strong leadership of a significant national initiative is essential to sustain technological capabilities and relative advantages over other countries. Any deviation from the established implementation path will necessitate a government update to assess the situation and provide a response to advance the government's objective of promoting artificial intelligence. It is recommended that the Prime Minister, who initiated the national program for artificial intelligence in 2018 as a basis for this decision, supervise the government's engagement through the National Security Council to ensure the effective implementation of the national program.
-  The Ministry of Innovation should collaborate with the Innovation Authority to facilitate the signing of necessary agreements that advance the computing infrastructure essential for advancing artificial intelligence in Israel.
-  Given the importance of developing large language models in Hebrew and Arabic, it is recommended that the Ministry of Innovation work jointly with the Innovation Authority, the Directorate of Defense, Research, & Development, and the National Digital Agency to advance this project and integrate it into government ministries and the public sector.





























-  Given concerns regarding the insufficiency of the grants program to address the recruitment challenges for new faculty in artificial intelligence, the required number of researchers should be determined, and the Planning and Budgeting Committee should explore alternative solutions for faculty recruitment, implementing them, according to the examination findings, in the future phases.
-  The Innovation Authority and the Planning and Budgeting Committee should establish control mechanisms focusing on data collection and analysis to assess the impact and effectiveness of scholarship distribution on enhancing and expanding human capital in artificial intelligence.
-  The Ministry of Innovation should investigate the reasons behind the limited execution of components from the initial phase of the human capital program and ensure comprehensive implementation in subsequent phases. Recognizing that the primary barrier to leveraging capabilities in artificial intelligence is human capital, the Ministry of Innovation, in collaboration with the Planning and Budgeting Committee, should develop a comprehensive strategy for increasing the scope of research and the number of faculty and researchers in artificial intelligence.
-  The Ministry of Innovation and the Ministry of Justice should cooperate to update regulatory principles in line with technological advancements and the standards established in the signed international treaty and bring them for government approval. They should also assess the necessity of promoting legislation akin to the practices in the European Union or advancing sector-specific regulation based on concrete risk, as is customary in the United States, United Kingdom, and Australia. In any case, regulatory frameworks are imperative to safeguard state and citizen security against the misuse of artificial intelligence capabilities.
-  Having received the mandate from the government to lead and advance the artificial intelligence sector in Israel, the Ministry of Innovation should implement the second phase as outlined in the government resolution, monitor the timelines and content of its execution in collaboration with the Telem Forum and other relevant government ministries and bodies engaged in the promotion and integration of this field in Israel.
-  It is recommended that the Ministry of Innovation, with the Ministry of Education, incorporate educational initiatives into the national artificial intelligence program by developing curricula that enhance data literacy. Moreover, following the completion of the subcommittee's work established by the Director General of the Ministry of Education to advance artificial intelligence, the Ministry of Education should formalize its integration into all educational institutions' curricula through a circular from the Director General, formulating a multi-year implementation plan.





## The Implementation Status of the First Phase Main Projects

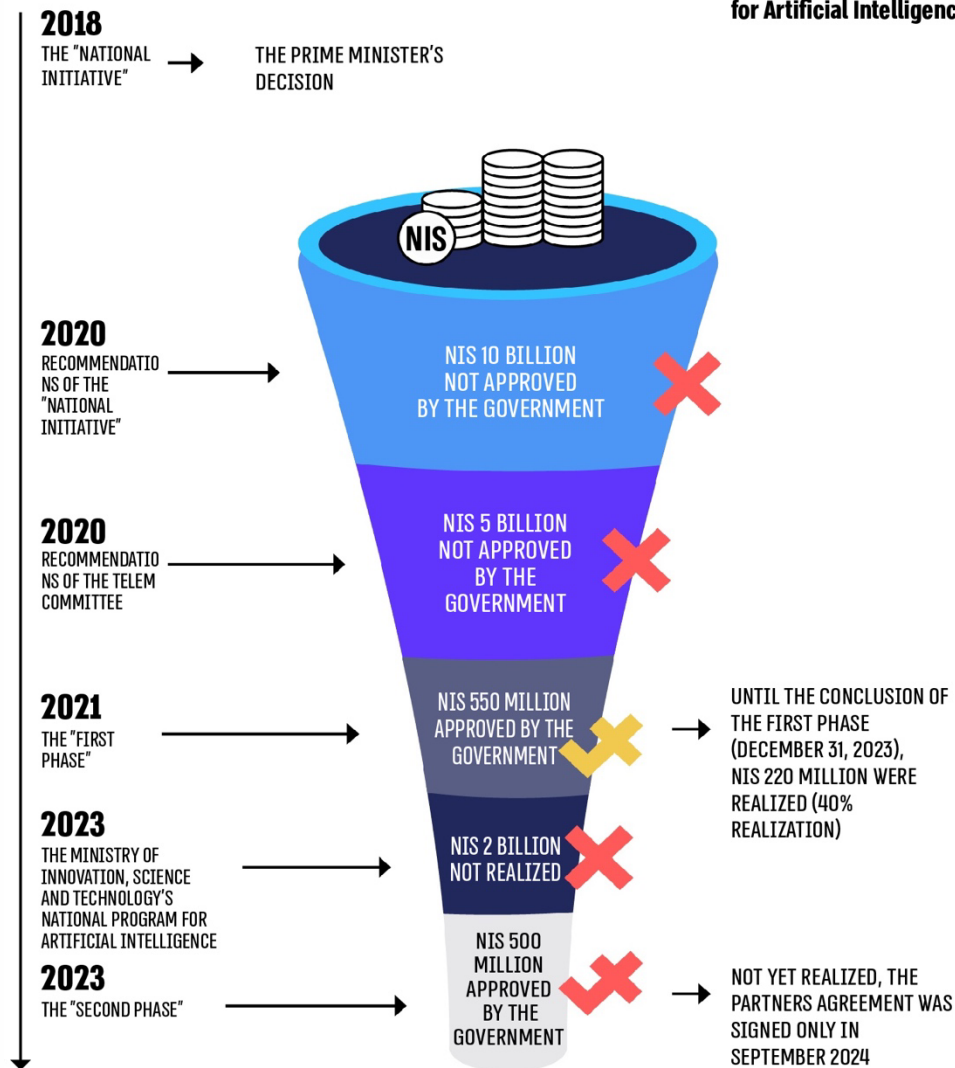
Regulation	Human capital	High Performance Computing (super-computer)	Natural Language Processing
<b>The Ministry of Innovation, Science and Technology</b>   Policy, regulations and ethics principles document	<b>Planning and Budgeting Committee</b>   Scholarships for doctoral candidates	<b>DDR&amp;D</b>   Large module training infrastructure	<b>DDR&amp;D</b>   Large Language Module in Hebrew and Arabic (LLM)
	<b>Planning and Budgeting Committee</b>   Scholarships for students	<b>The Innovation Authority</b>   Scientific calculation infrastructure	<b>The Innovation Authority</b>   Call for bids for language processing databases, models and tools
	<b>Planning and Budgeting Committee</b>   Hiring of faculty in the field of CORE AI	<b>The Innovation Authority</b>   Lab infrastructure for research and development	<b>DDR&amp;D</b>   Hebrew – Arabic translations
	<b>Planning and Budgeting Committee</b>   Dedicated research grants for research in CORE AI		<b>The Ministry of Innovation, Science and Technology</b>   Applicable research in academia
			<b>The Innovation Authority</b>   TRUST AI

Not Executed  Partially Executed  Executed 



## The Budgetary and Substantial Development of the National Program for Artificial Intelligence

### The National Program for Artificial Intelligence





## Summary

The scientific and technological leadership of the State of Israel is a fundamental pillar of its national security, economic resilience, and the well-being of its citizens. Israel's leadership in these domains strategically compensates for its lack of natural resources and limited human capital compared to other nations. The artificial intelligence revolution has transitioned from a futuristic concept to a core innovative technology impacting numerous facets of contemporary life, serving as a central focal point for international competition across various fields, including science, economics, industry, security, health, education, and employment.

According to the report, while Israel recognized already in 2018 that the technological sector was on the brink of a significant revolution, and the Prime Minister acknowledged the necessity of preparing and implementing a comprehensive national plan on the subject, since that time, the government has failed to lead and implement strategies for approving a broad, long-term national plan and has not initiated its implementation, nor continuously supervised to ensure the necessary progress. Consequently, Israel's standing in the international arena has begun to erode.

Despite the Prime Minister's 2018 decision to establish the "National Initiative" and despite the Telem Committee, a professional review committee appointed to examine the acceleration required for the development of artificial intelligence, having determined in 2020 that a national program in artificial intelligence and data science is critical for the resilience of the State of Israel, there remains no national program approved and budgeted by the government as of 2024. In 2018-2023, two significant plans were developed to advance the field of artificial intelligence at the national level: "National Initiative" and the Telem Committee program; However, these initiatives have either been abandoned or progressed minimally. The audit indicated that the 2021 agreement between the head of the National Security Council and the then-Minister of Innovation that her ministry shall be given overall responsibility and powers for managing the national program and coordinating the government's actions, as supported by the government's resolution, has not been implemented. Furthermore, the National Program formulated by the Ministry of Innovation has not been advanced, and since the change in government in December 2022, the Ministry of Innovation has focused solely on specific areas.

Consequently, about six years after the Prime Minister's decision, and given the accelerated development of artificial intelligence technology globally, Israel lacks a comprehensive long-term national strategy, and the government has not approved a comprehensive and specific master plan for implementation. The government's endorsement of programs has been sporadic, slow implementation, and has not adhered to established timelines. Additionally, the government did not approve the principles of policy, regulation, and ethics regarding artificial intelligence developed by the Ministry of Innovation and the Ministry of Justice, leaving crucial elements unanchored in legislation or sectoral regulation.



It is evident that while the state identified and analyzed the need promptly, it has struggled for several years to make effective decisions corresponding to that need and to implement them accordingly.

To uphold Israel's technological and scientific superiority in artificial intelligence, deemed a national priority, the Ministry of Innovation should lead the government policy, aligning its actions with the government's previous resolutions and the agreement between the then-Minister and the National Security Council. This entails finalizing the national strategic program initiated in 2022, which should encompass a clear vision, milestones, a detailed action plan specifying governmental responsibility for each action direction, implementation timelines, and an aligned budget. Additionally, the Ministry should establish a framework for a periodic assessment of the program's compliance with the outlined objectives and an individual evaluation of the defined actions, including necessary updates. In this context, it must review, among other factors, the current administrative structure responsible for implementing the initiatives approved by government resolutions, which, as of the audit end date, operates voluntarily and without budgetary authority.

The Ministry of Innovation, Science, and Technology should fulfill its responsibility by upholding the government's resolutions. Strong leadership of a significant national program is essential for sustaining Israel's technological capabilities and relative advantage over other nations. Any deviation from the established implementation course necessitates a governmental update to assess the situation and respond accordingly to promote artificial intelligence initiatives further.

It is recommended that the Prime Minister, who initiated the move to advance the national program in artificial intelligence in 2018, monitor the progress of governmental actions in this regard through the National Security Council, guaranteeing the practical implementation of a significant national plan.